SSH-Honeypots und neue Schutzmaßnahmen gegen Brute Force Angriffe

Andreas Bunten
andreas@bunten.de
Controlware GmbH, Waldstraße 92, 63128 Dietzenbach

Torsten Voss
voss@dfn-cert.de
DFN-CERT Services GmbH, Sachsenstraße 5, 20097 Hamburg

Zusammenfassung

Brute Force Angriffe gegen SSH-Server, bei denen versucht wird offensichtliche Passwörter zu erraten sind lange bekannt, aber noch immer ein Problem. Um Anmeldeversuche von bereits bekannten Angreifer-Systemen zu unterbinden, verwalten verschiedene Organisationen Listen von IP-Adressen, denen der Zugriff auf den SSH-Dienst untersagt wird. Da manche angreifende Systeme ihre IP-Adresse wechseln können (z.B. im Einwahlnetz eines Providers), werden diese Angreifer nicht wiedererkannt. Weiterhin steigt durch einen IP-Wechsel die Chance legitime Benutzer zu sperren, die zufällig die IP-Adresse eines Angreifers erhielten.

Die Autoren haben verschiedene Honeypots betrieben, um das Vorgehen der Angreifer besser zu verstehen und führten dabei zeitnah Port Scans gegen die angreifenden Systeme durch. Darauf aufbauend wurden verschiedene Merkmale extrahiert, die alternativ oder ergänzend zur IP-Adresse verwendet werden können, um ein angreifendes System wiederzuerkennen. Die Merkmale und Kombinationen daraus wurden auf Basis der Daten aus 12858 Angriffen ausgewertet, die zwischen dem 15. Februar und dem 15. November 2012 mit Hilfe der Honeypots aufgezeichnet wurden.

Der Hostkey des SSH-Dienstes hat sich als eines der besten Merkmale herausgestellt, um angreifende Systeme wiederzuerkennen. Der Hostkey kann zusammen mit der IP-Adresse des angreifenden System als kombiniertes Merkmal verwendet werden, um mehr Angreifer zu erkennen oder alternativ, um sicherer zu erkennen. Ein weiteres Ergebnis der Untersuchung ist, dass eine Sperrliste lediglich die Angreifer-Daten der letzten drei Wochen vorhalten muss. Werden mehr Daten gesammelt, so steigt die Erkennungsrate der angreifenden Systeme nur noch marginal.

1 Motivation

Wenn man ein UNIX-basiertes System am Internet betreibt, sieht man viele Anmeldeversuche von fremden Systemen. Verbindet man ein Test-System mit schwachem Root-Passwort mit dem Netz, findet man schnell heraus, dass die Anmeldeversuche keine Versehen sind, sondern Angriffe durch die der Server kompromittiert werden soll.

Man nennt diese Angriffe SSH Account Probes oder auch Brute Force Angriffe. Dahinter steht, dass Angreifer sich zum Opfer-System verbinden und eine Reihe von typischen Passwörtern durchprobieren. Grundsätzlich ist dies ein recht simpler Angriff und er ist leicht zu verhindern: Verwenden alle Benutzer starke Passwörter, gibt es kein Problem. Leider ist dies nicht immer einfach durchzusetzen und alternative Lösungen wie Zwei-Faktor-Authentifikation sind manchen Organisationen zu teuer, um sie flächendeckend einzusetzen.

Da sich je nach Ausgangslage dadurch ein gewisser Prozentsatz an erfolgreichen Angriffen schwer verhindern lässt, sind manche Organisationen und Open Source Projekte dazu übergegangen Sperrlisten für sich verbindende Systeme anzulegen. Diese umfassen in der Regel IP-Adressen, von denen bereits Brute Force Angriffe verzeichnet wurden (siehe z.B. [1]). Leider ist dabei nicht immer klar, woher die Einträge auf der Liste kommen und wie lange sie schon auf der Liste sind. Man muss davon ausgehen, dass die Angreifer potentiell ihre IP-Adressen ändern können. Wird eine IP-Adresse zu lange auf der Sperrliste geführt, steigt aufgrund von Neubelegung der IP-Adresse die Chance, legitime Benutzer auszusperren. Im Rahmen der Untersuchung von SSH-Angriffen mit Hilfe von Honeypots stellte sich den Autoren die Frage, ob es nicht geeignetere Methoden gibt, angreifende Systeme wiederzuerkennen als über ihre aktuelle IP-Adresse.

2 SSH-Honeypots

Bei der Aufklärung einer Vielzahl von SSH-Angriffe fiel den Autoren auf, dass immer wieder die gleichen Tools und Skripte zum Einsatz kommen. Weiterhin wirkte es so, als ob ein Großteil der Angriffe von wenigen Personen durchgeführt wurde. Dies war der Ausgangspunkt, um SSH-Angriffe mit Hilfe von Honeypots näher zu untersuchen.

Lance Spitzner vom Honeynet Project definiert einen Honeypot als eine Ressource, deren Wert darin liegt, von einem Angreifer missbraucht zu werden [2][3]. Für die Untersuchung der SSH-Angriffe wurden verschiedene Arten von Honeypots verwendet. Um erste Informationen über die SSH-Angreifer zu erlangen, wurden zunächst Low Interaction Honeypots eingesetzt, die Anmeldeversuche der Angreifer protokollieren, aber keine weitere Interaktion zulassen. Virtuelle Honeypots auf Basis der Software Kippo [4] dienten dazu, den Angreifern nach vermeintlich erfolgreicher Anmeldung eine Shell-Session vorzutäuschen. Die Simulation des kompromittierten Servers durch Kippo ist begrenzt, aber erlaubte erste Einblicke in das Vorgehen der Angreifer nach einer Kompromittierung. Um tieferes Verständnis für den vollständigen Angriffsablauf zu erlangen, wurden schließlich High Interaction Honeypots eingesetzt [5].

Alle Honeypot-Systeme melden einen beginnenden Angriff an zentral betriebene Server. Dort wird protokolliert und zusätzlich ein Port Scan mit Dienst-Erkennung gegen das angreifen-

de System durchgeführt. Grundsätzlich sind Port Scans nicht illegal, aber werden in der Regel zumindest als unfreundlicher Akt oder Angriffsvorbereitung gesehen. Die Autoren haben sich nach reiflicher Abwägung dafür entschieden Port Scans gegen nachweislich angreifende Systeme durchzuführen, um mehr Informationen zum Schutz vor SSH-Angriffen sammeln zu können. Zu den bereits veröffentlichen Ergebnissen des Einsatzes von Honeypots gehört, dass die eigentlichen Passwort-Rate Angriffe in der Regel von kompromittierten Systemen aus durchgeführt werden [6]. Diese Systeme wurden wahrscheinlich auf dem gleichen Weg angegriffen und bieten entsprechend einen öffentlichen SSH-Dienst an.

E. Alata, V. Nicomette, M. Kaâniche, M. Dacier und M. Herrb verwendeten 2006 eine Kombination aus Low Interaction und High Interaction Honeypots, um das Angreifer-Verhalten genauer zu untersuchen. Neben SSH-Servern wurden weitere Dienste für die Angreifer simuliert [7]. Daniel Ramsbrock, Robin Berthier und Michel Cukier untersuchten 2007 neben den Anmeldeversuchen bei SSH-Angriffen auch die typischen Aktionen der Angreifer nach erfolgreichem Login auf dem kompromittierten System [8]. Jim Owens and Jeanna Matthews untersuchten 2008 die im Rahmen von Brute Force Angriffen eingesetzten Passwort-Listen und stellen fest, dass auch nicht triviale Passwörter Gefahr laufen erraten zu werden [9]. Dave Woutersen und Dave De Coster haben 2010 SSH-Angriffe mit Hilfe der Kippo Honeypot Software untersucht und sind wie die Autoren zu dem Ergebnis gekommen, dass die angreifenden Systeme in der Regel kompromittierte Server darstellen [10]. Manche Aspekte des Vorgehens der Angreifer wurden damit bereits ausgiebig untersucht. Die vorgeschlagenen Schutzmechanismen beschränken sich aber in der Regel auf die Durchsetzung von effektiven Passwort-Policies. Die Autoren untersuchten den bestehenden pragmatischen Ansatz zum Schutz durch Sperrlisten auf Basis von IP-Adressen und machen Vorschläge zur Verbesserung.

3 Merkmale zur Wiedererkennung der Angreifer

Die im Rahmen des Honeypot-Einsatzes und durch Port Scans gesammelten Daten können einen Grundstein für eine effizientere Wiedererkennung von Systemen bilden, die bereits als Angreifer identifiziert wurden. Auf Basis der erhobenen Daten sind verschiedene Merkmale denkbar.

3.1 IP-Adresse

Die IP-Adresse des angreifenden Systems wird aktuell von verschiedenen Projekten als Merkmal verwendet. Der Angriff mit der ID 214794 vom 17. November 2012 wurde beispielsweise von der IP-Adresse `201.57.xx.xx` aus durchgeführt. Die letzten beiden Bytes wurden zur Darstellung im Artikel anonymisiert, aber wird für den Vergleich der Merkmale in Originalform verwendet.

3.2 Dienst-Profil aus Port Scan

Aus den Ergebnissen des Port Scans kann ein Profil der auf dem angreifenden System erreichbaren Dienste erzeugt werden. Das System, welches den Angriff 214794 durchgeführt hat, besaß 11 erreichbare Dienste (siehe Abbildung 1).

port	protocol	anwendung	version
10000	tcp	http	MiniServ 1.570 Webmin httpd
6969	tcp	ssh	SCS sshd 2.0.13 protocol 1.5
3128	tcp	http-proxy	Squid webproxy 2.7.STABLE9
993	tcp	imap	Dovecot imapd
443	tcp	http	Apache httpd 2.2.16 (Debian)
143	tcp	imap	Dovecot imapd
111	tcp	rpcbind	
80	tcp	http	Apache httpd 2.2.16 (Debian)
53	tcp	domain	ISC BIND 9.7.3
25	tcp	smtp	Postfix smtpd
22	tcp	ssh	OpenSSH 5.5p1 Debian 6+squeeze1 protocol 2.0

Abbildung 1: Die erreichbaren Ports der Quelle des Angriffs 214794.

Als Merkmal für die Wiedererkennung von bekannten Angreifern werden die Port-Nummer (z.B. 22), das IP-Protokoll (z.B. TCP) und das erkannte Anwendungs-Protokoll (z.B. SSH) verwendet. D.h. ein System wird wiedererkannt, wenn es die gleichen Dienste anbietet.

3.3 SSH Hostkeys

Durch die Dienst-Erkennung im Rahmen der Port Scans werden je nach Dienst weitere Informationen erlangt. Bietet das angreifende System selbst einen SSH-Dienst an, wird der Fingerprint des vom SSH-Server eingesetzten SSH Hostkey ermittelt. Dieser kann ebenfalls als Merkmal verwendet werden. In Abbildung 2 sind die im Angriff 214794 ermittelten Hostkeys zu sehen.

```
1024 5a:8f:2b:04:25:75:40:2a:69:63:b5:b5:01:8c:dd:b1 (DSA)
2048 16:1c:50:f4:86:a7:a0:df:c1:dc:37:4e:d6:a0:b8:22 (RSA)
1024 dc:cd:da:72:fe:6e:db:70:ff:11:e5:cc:b4:27:80:80 (RSA1)
```

Abbildung 2: Die Hostkeys des Quell-Systems des Angriffs 214794.

Es wird der eigentliche Fingerprint des Hostkeys ohne Informationen zum Port, Protokoll, kryptographischen Algorithmus und der Schlüssellänge verwendet. Im Falle des Angriffs 214794 ergaben sich entsprechend drei Fingerprints als Merkmale.

3.4 Eindeutigkeit der Merkmale

Dienst-Profile kommen kaum als alleiniges Merkmal in Frage, da man damit rechnen müsste, dass es zu vielfachen Falschmeldungen kommt. Würde z.B. ein Angreifer registriert, der

nur einen SSH-Dienst betreibt, würden danach alle Systeme als Angreifer erkannt werden, die ebenso nur einen SSH-Dienst anbieten. Sinnvoll ist dieses Merkmal gegebenenfalls in Kombination mit anderen Merkmalen.

Eine stichprobenhafte Untersuchung der Daten ergab, dass keines der Merkmale eindeutig für eine Identifizierung eines Systems geeignet ist. Bei IP-Adresse angreifender Systeme ist dies noch leicht einzusehen, wenn man z.B. Angreifer-Systeme in DSL-Einwahlnetzen betrachtet, die regelmäßig vom Provider eine neue IP-Adresse erhalten.

Von den SSH Hostkeys könnte man annehmen, dass diese eindeutig sind. Die gesammelten Daten wiederlegen dies allerdings klar. Speziell drei verschiedene SSH Hostkeys wurden in über 500 unterschiedlichen Angriffen beobachtet (siehe Abbildung 3). Dabei wurden IP-Adressen verwendet, die über die ganze Welt vertreut sind. Daher kann es sich kaum um ein einzelnes System handeln.

```
1024 dc:cd:da:72:fe:6e:db:70:ff:11:e5:cc:b4:27:80:80 (RSA1)
1024 20:e4:a9:50:e3:40:f4:54:cc:d4:47:02:bc:99:7b:f3 (DSA)
1040 1b:7e:77:e2:9e:2d:9d:4c:38:43:83:e6:37:2d:4b:ed (RSA)
```

Abbildung 3: Die am meisten aufgetretenen SSH Hostkeys.

Bei genauerer Betrachtung ergaben sich eine Reihe von Umständen, die eine mehrfache Verwendung von SSH Hostkeys begründen können. Hier sind exemplarisch drei aufgeführt:

Appliances: Manche Appliance-Hersteller liefern ihre Systeme mit identischen Schlüssel-Material für den SSH Remote-Zugang aus (siehe [11] als Beispiel). Werden diese kompromittiert und für Angriffe verwendet, oder - im Falle von NAT-Gateways - erfolgen die Angriffe von einem System hinter dem Gateway, so wird die Appliance auf einen Port Scan mit dem standardmäßig ausgelieferten SSH Hostkey antworten.

Kryptographische Fehler: Aufgrund von Fehlern bei der Implementierung oder aufgrund von fehlender Entropie bei der Schlüssel-Erzeugung kann es zu Generierung pathologischer Schlüssel kommen. Dies kann z.B. durch die Schlüssel-Erzeugung direkt beim ersten Start einer Netzwerk-Appliance vorkommen.

Malware: Aufgrund der Analyse der Honeypot-Daten kann geschlossen werden, dass zumindest ein Großteil der angreifenden Systeme selbst kompromittiert wurde. Einige der Systeme wurden von den Angreifern wahrscheinlich mit einer Backdoor versehen, um auch in Zukunft wieder Zugang zu erhalten auch wenn die Schwachstelle geschlossen wurde. Häufig wird ein SSH-Server auf einem untypisch hohen Port als Backdoor verwendet. Verwendet eine Angreifer-Gruppe ein bestimmtes SSH-Server Paket als Backdoor, so wird dort wahrscheinlich ein bereits erzeugter Key enthalten sein.

Alle hier aufgeführten Gründe für ein mehrfaches Auftreten von SSH Hostkeys stellen eine direkte Gefahr oder zumindest ein Bruch mit gängigen Security Best Practice dar.

4 Vergleich der Merkmale

Um die Qualität der Merkmale zur Wiedererkennung der angreifenden Systeme zu vergleichen werden die Ergebnisse des Honeypot-Betriebs und die aufgezeichneten Port Scans untersucht. Zu einem Angriff kann nachträglich bestimmt werden, ob das angreifende System anhand eines bestimmten Merkmals wiedererkannt worden wäre. Dazu wurden jeweils die Merkmale der Angriffe einer variablen Anzahl von zurückliegenden Tagen betrachtet. Die Anzahl der Tage wird im Folgenden als das Gedächtnis bezeichnet.

Um einen sinnvollen Vergleich der Merkmale zu ermöglichem, wurden nur Angriffe betrachtet zu denen unmittelbar ein Port Scan erfolgreich durchgeführt wurde. Es wurden insgesamt 12858 Angriffe im Zeitraum vom 15. Februar bis zum 15. November 2012 einbezogen. Um ein Gedächtnis mit maximal 60 Tagen zu ermöglichen, wurden die Daten bis zum 15. April lediglich für die Vorbefüllung des Gedächtnis-Speichers verwendet.

Abbildung 4 zeigt die tägliche Erfolgsrate im untersuchten Zeitraum für die verschiedenen Merkmale. Die Erfolgsrate gibt prozentual die Angriffe des jeweiligen Tages an, die aufgrund des verwendeten Merkmals bei einem Gedächtnis von 30 Tagen als Angriff erkannt worden ist. Die Rate mit der Angreifer wiedererkannt werden schwankt erwartungsgemäß von Tag zu Tag. Die Erkennung über das Dienst-Profil scheint ein deutlich besseres Ergebniss zu liefern als die beiden anderen Merkmale. Dies ist nicht verwunderlich, da das Dienst-Profil alleine wahrscheinlich zu einer hohen falschen Erkennungsrate führt und nicht alleine eingesetzt werden sollte.

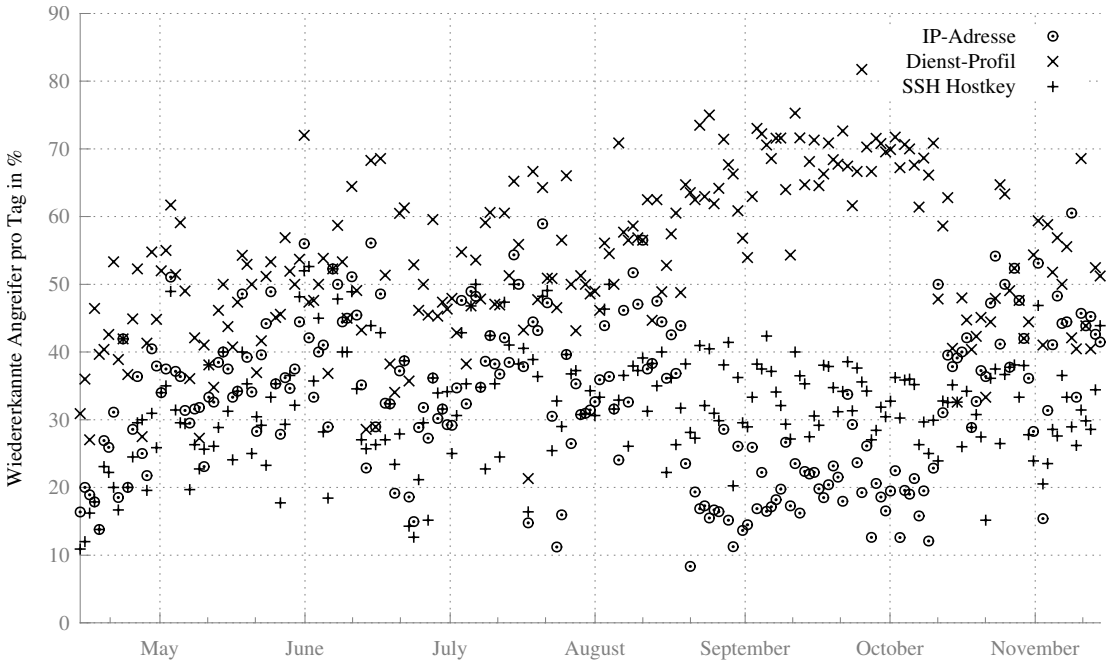

Abbildung 4: Die täglichen Wiedererkennungsraten der verschiedenen Merkmale bei einem Gedächtnis von 30 Tagen.

Bei genauer Betrachtung von Abbildung 4 fällt eine Besonderheit der Daten im September auf. Die Wiedererkennung der Angreifer durch IP-Adressen scheint sich stark zu verschlechtern

und die Wiedererkennung anhand des Dienst-Profils steigt an. Lediglich die Wiedererkennung durch das Merkmal SSH Hostkey scheint nicht betroffen zu sein. Eine Spur für die Erklärung kann in der Anzahl der unterschiedlichen IP-Adressen pro Tag gefunden werden, die als Angreifer registriert werden (siehe Abbildung 5). Über die zu erwartende tägliche Schwankung hinaus ist im September ein starker Anstieg der Anzahl der täglichen Angreifer IP-Adressen zu erkennen. Eine nähere Untersuchung der Rohdaten ergab keine definitive Klärung. Die Autoren gehen davon aus, dass der Effekt durch eine Serie von Attacken einer einzelnen Angreifer-Gruppe verursacht wurde. Dabei kamen Systeme zum Einsatz, die ihr IP-Adressen wechseln konnten, um so der Erkennung bzw. der Sperrung zu entgehen. Anhand des SSH Hostkey kann ein System dennoch wiedererkannt werden. Vermutlich waren die bei den Angriffen eingesetzten Systeme einheitlich konfiguriert. Dies erklärt den starken Anstieg der Erkennung durch Dienst-Profile, da so Systeme vermeintlich wiedererkannt werden, obwohl sie gerade den ersten Angriff durchführen.

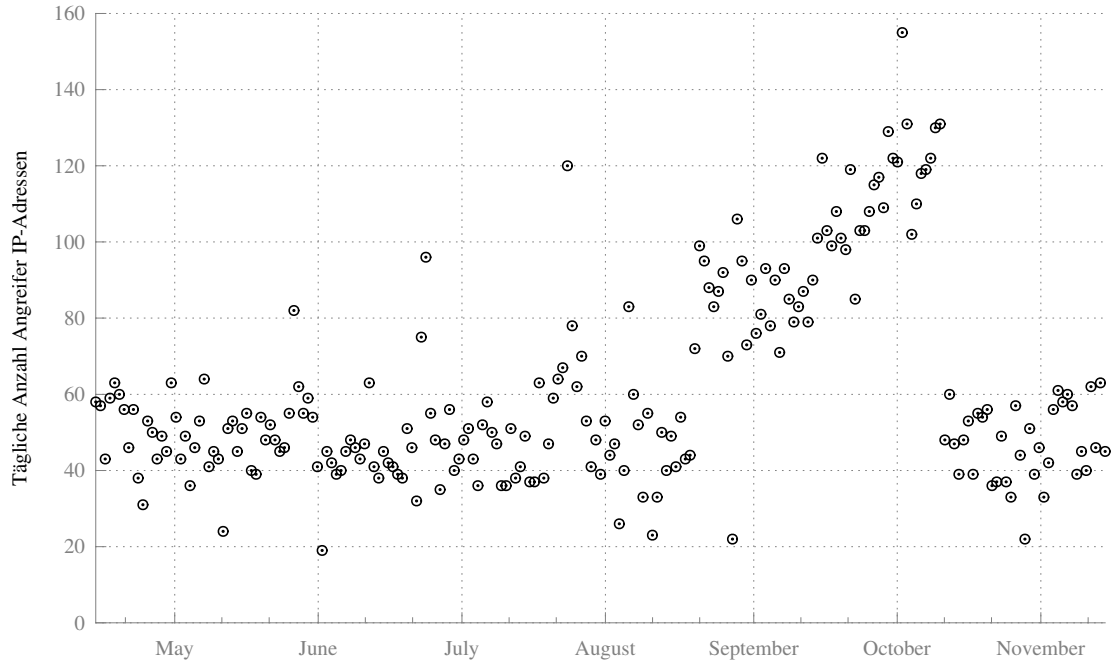

Abbildung 5: Die Anzahl der täglich registrierten unterschiedlichen IP-Adressen, von denen Angriffe ausgingen.

Die Schwankungen der täglichen Wiedererkennungsraten sind besser in den Histogrammen für die jeweiligen Merkmale zu erkennen (siehe Abbildung 6). Das Histogram für das Merkmal SSH Hostkey weist eine geringere Standardabweichung auf als die beiden anderen Histogramme. Die Wiedererkennungsrate schwankt damit deutlich weniger um den Mittelwert, wenn der SSH Hostkey als Merkmal verwendet wird.

Die SSH Hostkeys scheinen damit eine konstantere Wiedererkennung der angreifenden Systeme zu ermöglichen, wobei die eigentliche Erkennungsraten durch die IP-Adressen grob vergleichbar sind und die durch Dienst-Profile sogar deutlich besser sind.

Um den Einfluss der Länge des Gedächtnis zu untersuchen wurden für eine Gedächtnislänge eine mittlere Rate zur Wiedererkennung über den gesamten betrachteten Zeitraum gebildet.

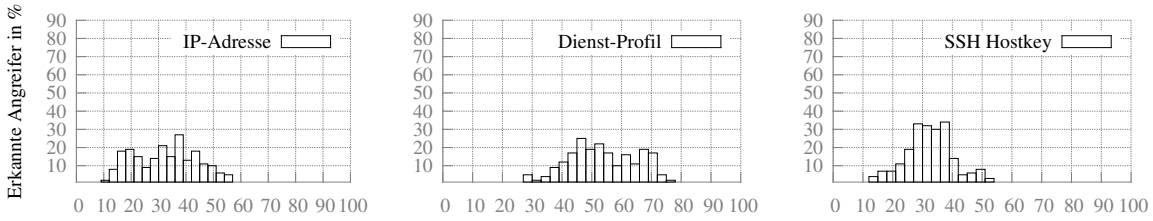

Abbildung 6: Histogramm der täglichen Wiedererkennungsraten der verschiedenen Merkmale in % bei einem Gedächtnis von 30 Tagen. Die Intervalle haben eine Größe von 3%.

In Abildung 7 sind diese Werte für die beiden Merkmale IP-Adresse und SSH Hostkey bei einer Gedächtnislänge von einem bis 60 Tage zusammen mit der absoluten und der relativen Standardabweichung abgetragen.

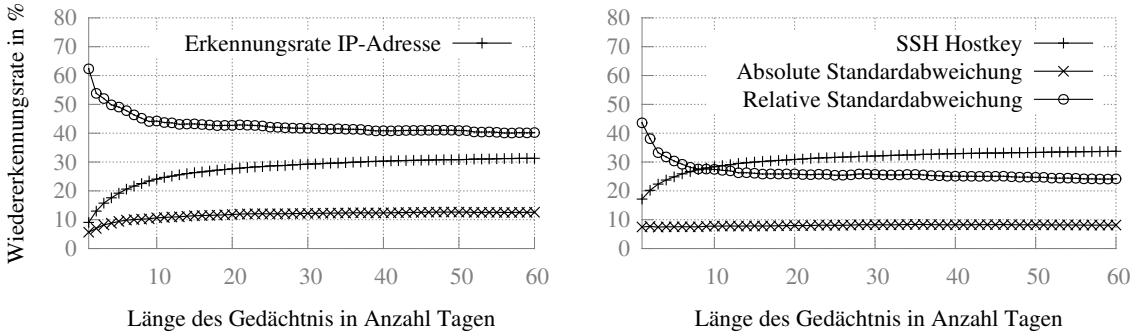

Abbildung 7: Die mittleren Wiedererkennungsraten für die Merkmale IP-Adresse und SSH Hostkey. Die Gedächtnislänge wird zwischen einem und 60 Tagen variiert. In jedem Graph ist zusätzlich die absolute und die relative Standardabweichung abgetragen.

Es ist zu erkennen, dass die Erkennungsrate zwar kontinuierlich mit der Länge des Gedächtnis ansteigt. Die Steigerung ab dem 20. Tag erfolgt aber nur noch sehr langsam. Weiterhin ist zu sehen, dass die Wiedererkennung von Angreifern über SSH Hostkeys geringfügig erfolgreicher ist. Die absolute Standardabweichung gibt die Schwankung der täglichen Wiedererkennungsraten an und liegt beim Merkmal IP-Adresse auf einem deutlich höheren Niveau. Die relative Standardabweichung gibt die tägliche Schwankung der Wiedererkennungsrate skaliert zur tatsächlichen mittleren Rate wieder. Für beide Merkmale sinkt die relative Standardabweichung bei steigendem Gedächtnis, was grundsätzlich zu erwarten war. Beim Merkmal IP-Adresse liegt die relative Standardabweichung allerdings auf einem deutlich höheren Niveau. Demnach kann von einer etwas besseren Mindest-Erkennungsrate ausgegangen werden, wenn der SSH Hostkey als Merkmal verwendet wird.

5 Kombination der Merkmale

Eine oder/und-Verknüpfung unterschiedlicher Merkmale erlaubt eine freizügigere Wiedererkennung der Angreifer oder eine zusätzlichere Absicherung, dass keine Falschmeldung vor-

liegt. Da das Dienst-Profil nicht geeignet ist, um ein sich verbindendes System als Angreifer zu klassifizieren, ergeben sich vier Kombinationen:

SSH Hostkey und Dienst-Profil: Das sich verbindende System wird als Angreifer wiedererkannt, wenn bereits ein Angriff protokolliert wurde, bei dem der gleiche SSH Hostkey vorgefunden wurde und das gleiche Dienst-Profil vorlag.

IP-Adresse und Dienst-Profil: In dieser Kombination ist für eine Wiedererkennung des Angreifers erforderlich, dass die IP-Adresse bereits von einem vorherigen Angriff bekannt ist und das Dienst-Profil ebenfalls mit diesem Angriff übereinstimmt.

SSH Hostkey und IP-Adresse: In dieser Merkmals-Kombination muss die IP-Adresse und der SSH Hostkey bereits aus einem vorherigen Angriff bekannt sein, damit eine Verbindung als Angriff von einem bekannten System klassifiziert wird.

SSH Hostkey oder IP-Adresse: Um angreifende Systeme leichter wiederzuerkennen und nicht um die Möglichkeit von Falschmeldungen zu verringern, kann der SSH Hostkey oder die IP-Adresse verwendet werden. Stimmt nur ein Merkmal überein, wird die Verbindung als Angriff erkannt.

In Abbildung 8 ist das Ergebnis der Auswertung der gleichen Test-Daten mit den Merkmals-Kombinationen zu sehen.

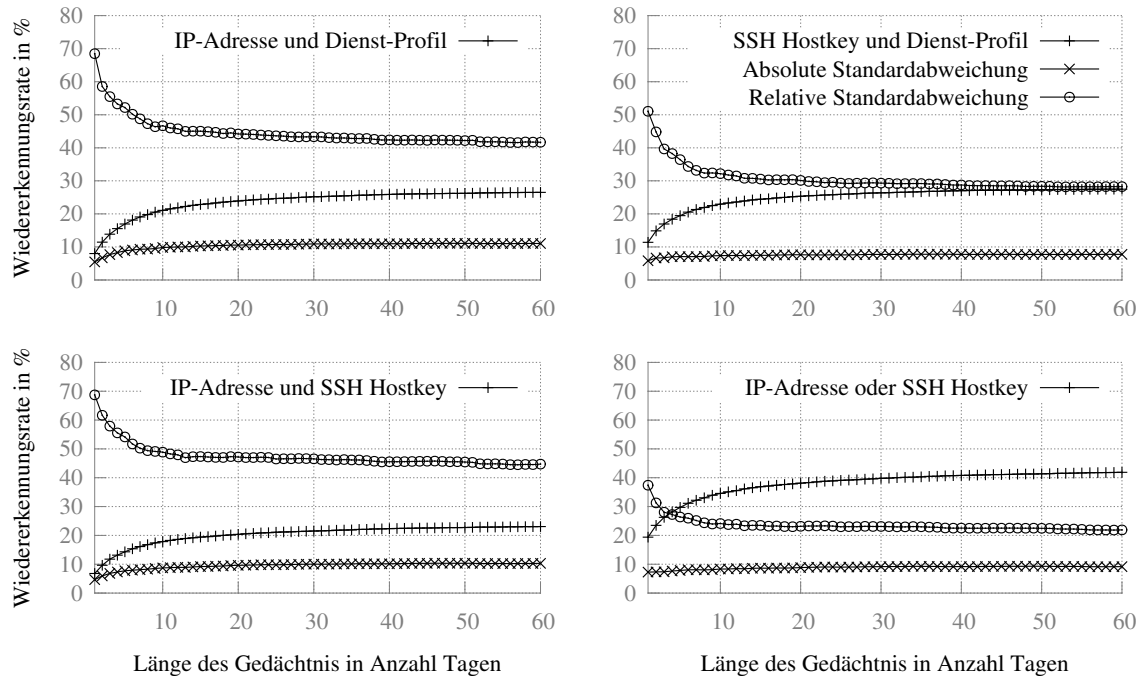

Abbildung 8: Die mittleren Wiedererkennungsraten für kombinierte Merkmale. Die Gedächtnislänge wird zwischen einem und 60 Tagen variiert. In jedem Graph ist zusätzlich die absolute und die relative Standardabweichung abgetragen.

Sowohl die Kombination IP-Adresse und Dienst-Profil wie IP-Adresse und SSH Hostkey haben eine überraschend hohe relative Standardabweichung von über 40% selbst im konvergenten Bereich - d.h. mit einem Gedächtnis von mindestens 20 Tagen. Die Schwankungen in der

Erkennungsrate sind damit höcher als bei den anderen Kombinationen. Etwas überraschend ist die Kombination SSH Hostkey und Dienst-Profil nicht so erfolgreich wie der SSH Hostkey alleine. Dies ist erneut eine Bestätigung dafür, dass der Host Key kein eindeutiges Identifikationsmerkmal ist. Die alleine durch den Hostkey fälschlich als Angreifer identifizierten Systeme haben allerdings sehr wahrscheinlich eines der in Abschnitt 3.4 aufgelisteten Probleme.

Die Kombination IP-Adresse und SSH Hostkey ist die härteste Bedingung innerhalb dieses Vergleichs und schneidet entsprechend schlecht ab mit einer Wiedererkennungsrate von knapp über 20% im konvergenten Bereich. IP-Adressen oder SSH Hostkeys als Merkmal zu verwenden resultiert in der höchsten Wiedererkennungsrate von etwas mehr als 40% im konvergenten Bereich. Die relative Standardabweichung ist dabei mit etwas über 20% die niedrigste.

6 Bewertung der Ergebnisse und praktischer Einsatz

Die IP-Adresse des angreifenden Systems ist ein gutes Merkmal, um dieses später erneut zu erkennen. Der SSH Hostkey erwies sich in der Auswertung der Honeypot Ergebnisse und der Scan Daten allerdings als erfolgreicheres und stabileres Merkmal. Neben der Auswertung der Honeypot Ergebnisse und der Scan Daten sprechen weitere Gründe für die Verwendung von SSH Hostkeys zur Erkennung von bekannten Angreifer-Systemen:

- Da die angreifenden Systeme in der Regel auf dem gleichen Weg kompromittierte Server darstellen, kann man mit einem erreichbaren SSH-Dienst rechnen. Die Angreifer werden außerdem in den seltensten Fällen den Hostkey verändern, da dies eine Entdeckung wahrscheinlicher macht.
- Fälschlich anhand des Hostkey als Angreifer erkannte Systeme weisen wahrscheinlich ein anderes massives Sicherheitsproblem auf; z.B. könnte eine Backdoor mit einem Standard SSH Hostkey die Erkennung auslösen.
- Zur Bereinigung eines kompromittierten Servers gehört gemäß Best Practice der Austausch von kryptographischen Schlüsseln - also auch des Hostkeys. D.h. der bereinigte Server wäre automatisch nicht mehr auf einer Hostkey Sperrliste.

SSH Hostkeys können alleine oder zusammen mit IP-Adressen als besseres Merkmal zur Wiedererkennung angreifender Systeme eingesetzt werden. Um interessierte Systembetreiber einen Test zu ermöglichen, stellen die Autoren unter [12] eine regelmäßig aktualisierte Sperrliste von SSH Hostkeys und den Prototyp eines Skripts zum Test eines Systems bzgl. der Sperrliste zur Verfügung.

7 Ausblick

Es wurden Honeypots eingesetzt, um SSH-Angriffe zu analysieren und bessere Methoden zur Erkennung von bekannten Angreifer-Systemen zu finden. SSH Hostkeys haben sich als praktikables und zuverlässigeres Merkmal zur Erkennung von bekannten Angreifern herausgestellt.

SSH Hostkeys können alleine oder zusammen mit den IP-Adressen der Angreifer-Systemen eingesetzt werden.

Grundsätzlich lässt sich das Vorgehen über das Secure Shell Protokoll hinaus auf andere Dienste verallgemeinern, bei denen sich die Server auch gegenüber den Client-Systemen authentisieren. Auch hier können kryptographische Fingerprints zur Erkennung eingesetzt werden, wenn davon ausgegangen werden kann, dass der Dienst auch auf dem angreifenden System betrieben wird, weil dieses auf die gleiche Weise kompromittiert wurde.

Literatur

[1] Homepage des DenyH0st Projekt, `http://denyhosts.sourceforge.net/`, zuletzt besucht 2012-11-16

[2] Homepage des Honeynet Projekt, `http://honeynet.org/`, zuletzt besucht 2012-11-16

[3] Niels Provos und Thorsten Holz: *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*, Addison-Wesley Longman, 2007

[4] Homepage der Honeypot Software Kippo, `http://code.google.com/p/kippo/`, zuletzt besucht 2012-11-16

[5] Video eines Angriffs auf einen SSH High Interaction Honeypot, `http://bunten.de/ssh.html`, zuletzt besucht 2012-11-16

[6] Andreas Bunten und Torsten Voss: *Wie man SSH-Angreifern mit Linux Honeypots nachstellt*, Vortrag auf dem 18. Linux Tag in Berlin, Mai 2012

[7] E. Alata, V. Nicomette, M. Kaâniche, M. Dacier und M. Herrb: *Lessons learned from the deployment of a high-interaction honeypot*, Proceedings of the Sixth European Dependable Computing Conference (EDCC'06), 2006

[8] Daniel Ramsbrock, Robin Berthier und Michel Cukier: *Profiling Attacker Behavior Following SSH Compromises*, 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07), 2007

[9] Jim Owens und Jeanna Matthews: *A Study of Passwords and Methods Used in Brute-Force SSH Attacks*

[10] Dave Woutersen und Dave De Coster: *Kippo -> SSH Honeypot, Beyond the SSH Bruteforce Attacks*, Vortrag auf dem GovCERT.NL Symposium 2010

[11] Heise News Artikel: *SSH-Private-Key lässt Angreifer auf BIG-IP Appliances*: `http://www.heise.de/netze/meldung/SSH-Private-Key-laesst-Angreifer-auf-BIG-IP-Appliances-1616754.html`, zuletzt besucht 2012-11-16

[12] Andreas Bunten und Torsten Voss, *Prototyp der SSH Hostkey Sperrliste*: `http://bunten.de/ssh-hostkeys.html`