Your Home is My Castle
—
Angriff auf die Updates eines Heimrouters

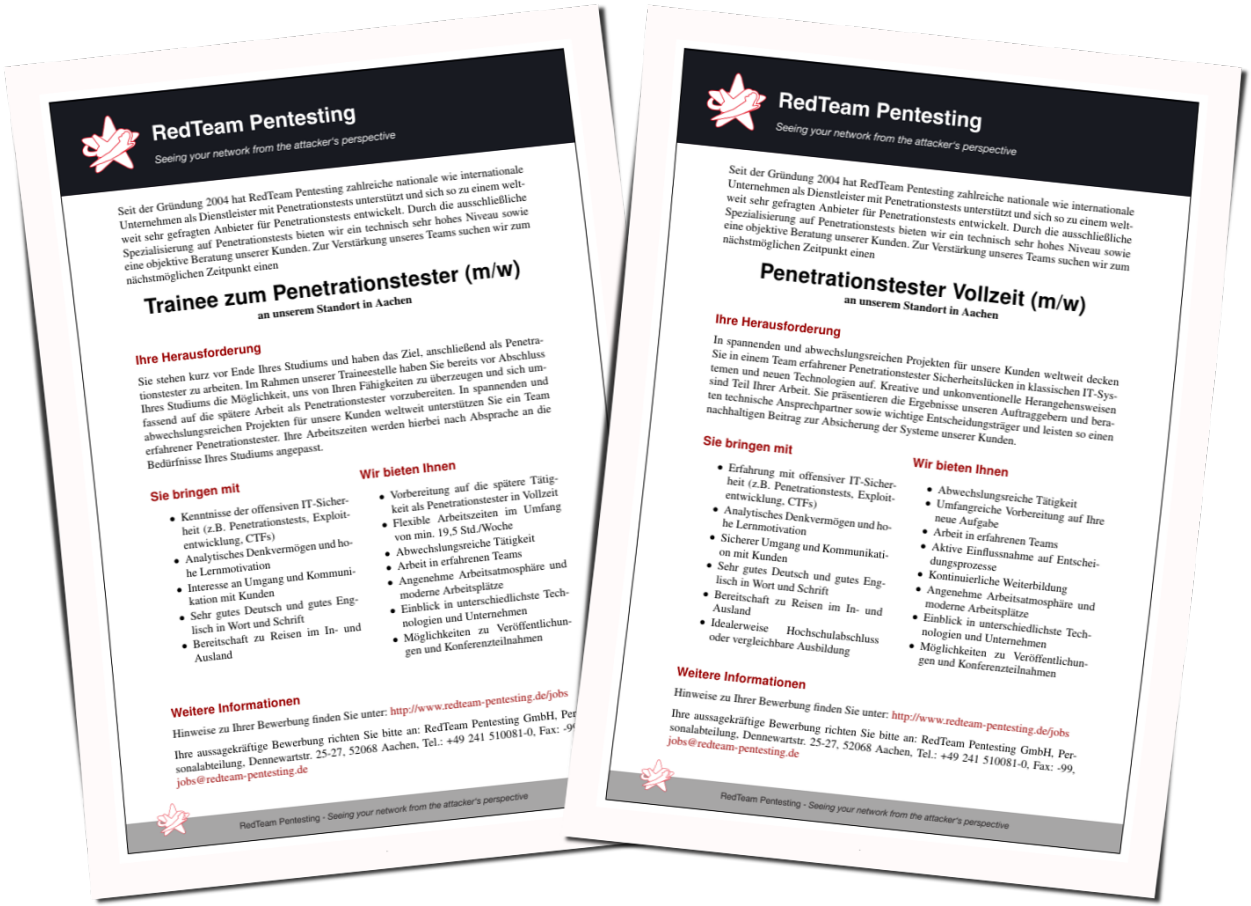
Hanno Heinrichs - RedTeam Pentesting GmbH
hanno.heinrichs@redteam-pentesting.de
https://www.redteam-pentesting.de

Cryptoparty des Open Source Arbeitskreises
18. Juni 2015, Aachen

RedTeam Pentesting, Daten & Fakten

- ★ Gegründet 2004
- ★ 10 Penetrationstester
- ★ Weltweite Durchführung von Penetrationstests
- ★ Spezialisierung ausschließlich auf Penetrationstests

Wir stellen ein!



RedTeam Pentesting

Seeing your network from the attacker's perspective

Seit der Gründung 2004 hat RedTeam Pentesting zahlreiche nationale wie internationale Unternehmen als Dienstleister mit Penetrationstests unterstützt und sich so zu einem weltweit sehr gefragten Anbieter für Penetrationstests entwickelt. Durch die ausschließliche Spezialisierung auf Penetrationstests bieten wir ein technisch sehr hohes Niveau sowie eine objektive Beratung unserer Kunden. Zur Verstärkung unseres Teams suchen wir zum nächstmöglichen Zeitpunkt einen

Trainee zum Penetrationstester (m/w)

an unserem Standort in Aachen

Ihre Herausforderung

Sie stehen kurz vor Ende Ihres Studiums und haben das Ziel, anschließend als Penetrationstester zu arbeiten. Im Rahmen unserer Traineestelle haben Sie bereits vor Abschluss Ihres Studiums die Möglichkeit, uns von Ihren Fähigkeiten zu überzeugen und sich umfassend auf die spätere Arbeit als Penetrationstester vorzubereiten. In spannenden und abwechslungsreichen Projekten für unsere Kunden weltweit unterstützen Sie ein Team erfahrener Penetrationstester. Ihre Arbeitszeiten werden hierbei nach Absprache an die Bedürfnisse Ihres Studiums angepasst.

Sie bringen mit

- Kenntnisse der offensiven IT-Sicherheit (z.B. Penetrationstests, Exploitentwicklung, CTFs)
- Analytisches Denkvermögen und hohe Lernmotivation
- Interesse an Umgang und Kommunikation mit Kunden
- Sehr gutes Deutsch und gutes Englisch in Wort und Schrift
- Bereitschaft zu Reisen im In- und Ausland

Wir bieten Ihnen

- Vorbereitung auf die spätere Tätigkeit als Penetrationstester in Vollzeit
- Flexible Arbeitszeiten im Umfang von min. 19,5 Std./Woche
- Abwechslungsreiche Tätigkeit
- Arbeit in erfahrenen Teams
- Angenehme Arbeitsatmosphäre und moderne Arbeitsplätze
- Einblick in unterschiedlichste Technologien und Unternehmen
- Möglichkeiten zu Veröffentlichungen und Konferenzteilnahmen

Weitere Informationen

Hinweise zu Ihrer Bewerbung finden Sie unter: http://www.redteam-pentesting.de/jobs

Ihre aussagekräftige Bewerbung richten Sie bitte an: RedTeam Pentesting GmbH, Personalabteilung, Dennewartstr. 25-27, 52068 Aachen, Tel.: +49 241 510081-0, Fax: -99, jobs@redteam-pentesting.de

RedTeam Pentesting - Seeing your network from the attacker's perspective

RedTeam Pentesting

Seeing your network from the attacker's perspective

Seit der Gründung 2004 hat RedTeam Pentesting zahlreiche nationale wie internationale Unternehmen als Dienstleister mit Penetrationstests unterstützt und sich so zu einem weltweit sehr gefragten Anbieter für Penetrationstests entwickelt. Durch die ausschließliche Spezialisierung auf Penetrationstests bieten wir ein technisch sehr hohes Niveau sowie eine objektive Beratung unserer Kunden. Zur Verstärkung unseres Teams suchen wir zum nächstmöglichen Zeitpunkt einen

Penetrationstester Vollzeit (m/w)

an unserem Standort in Aachen

Ihre Herausforderung

In spannenden und abwechslungsreichen Projekten für unsere Kunden weltweit decken Sie in einem Team erfahrener Penetrationstester Sicherheitslücken in klassischen IT-Systemen und neuen Technologien auf. Kreative und unkonventionelle Herangehensweisen sind Teil Ihrer Arbeit. Sie präsentieren die Ergebnisse unseren Auftraggebern und beraten technische Ansprechpartner sowie wichtige Entscheidungsträger und leisten so einen nachhaltigen Beitrag zur Absicherung der Systeme unserer Kunden.

Sie bringen mit

- Erfahrung mit offensiver IT-Sicherheit (z.B. Penetrationstests, Exploitentwicklung, CTFs)
- Analytisches Denkvermögen und hohe Lernmotivation
- Sicherer Umgang und Kommunikation mit Kunden
- Sehr gutes Deutsch und gutes Englisch in Wort und Schrift
- Bereitschaft zu Reisen im In- und Ausland
- Idealerweise Hochschulabschluss oder vergleichbare Ausbildung

Wir bieten Ihnen

- Abwechslungsreiche Tätigkeit
- Umfangreiche Vorbereitung auf Ihre neue Aufgabe
- Arbeit in erfahrenen Teams
- Aktive Einflussnahme auf Entscheidungsprozesse
- Kontinuierliche Weiterbildung
- Angenehme Arbeitsatmosphäre und moderne Arbeitsplätze
- Einblick in unterschiedlichste Technologien und Unternehmen
- Möglichkeiten zu Veröffentlichungen und Konferenzteilnahmen

Weitere Informationen

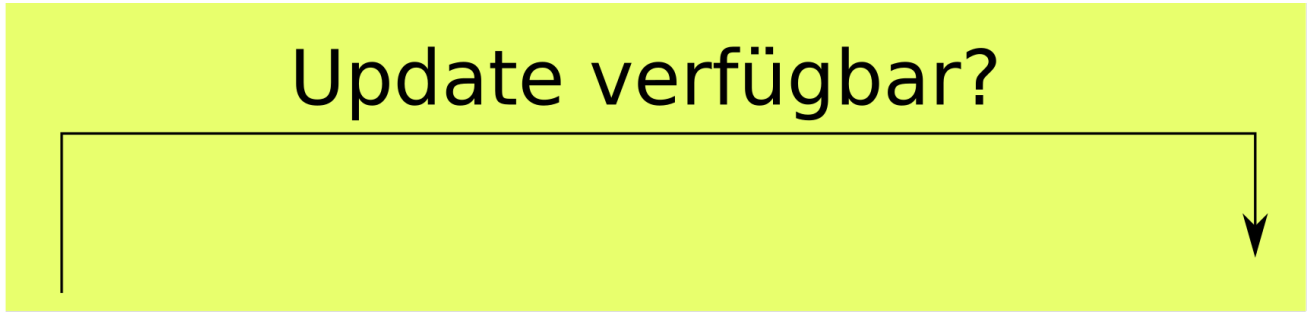
Hinweise zu Ihrer Bewerbung finden Sie unter: http://www.redteam-pentesting.de/jobs

Ihre aussagekräftige Bewerbung richten Sie bitte an: RedTeam Pentesting GmbH, Personalabteilung, Dennewartstr. 25-27, 52068 Aachen, Tel.: +49 241 510081-0, Fax: -99, jobs@redteam-pentesting.de

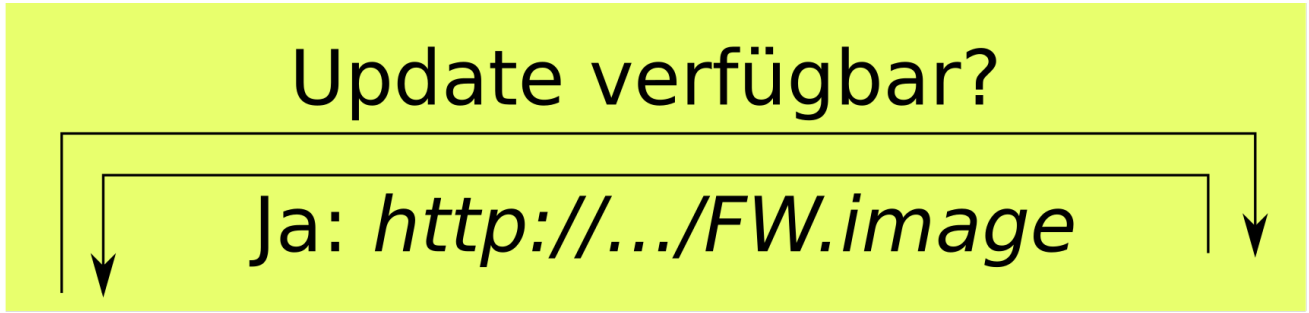
RedTeam Pentesting - Seeing your network from the attacker's perspective

⇒ `https://www.redteam-pentesting.de/jobs`

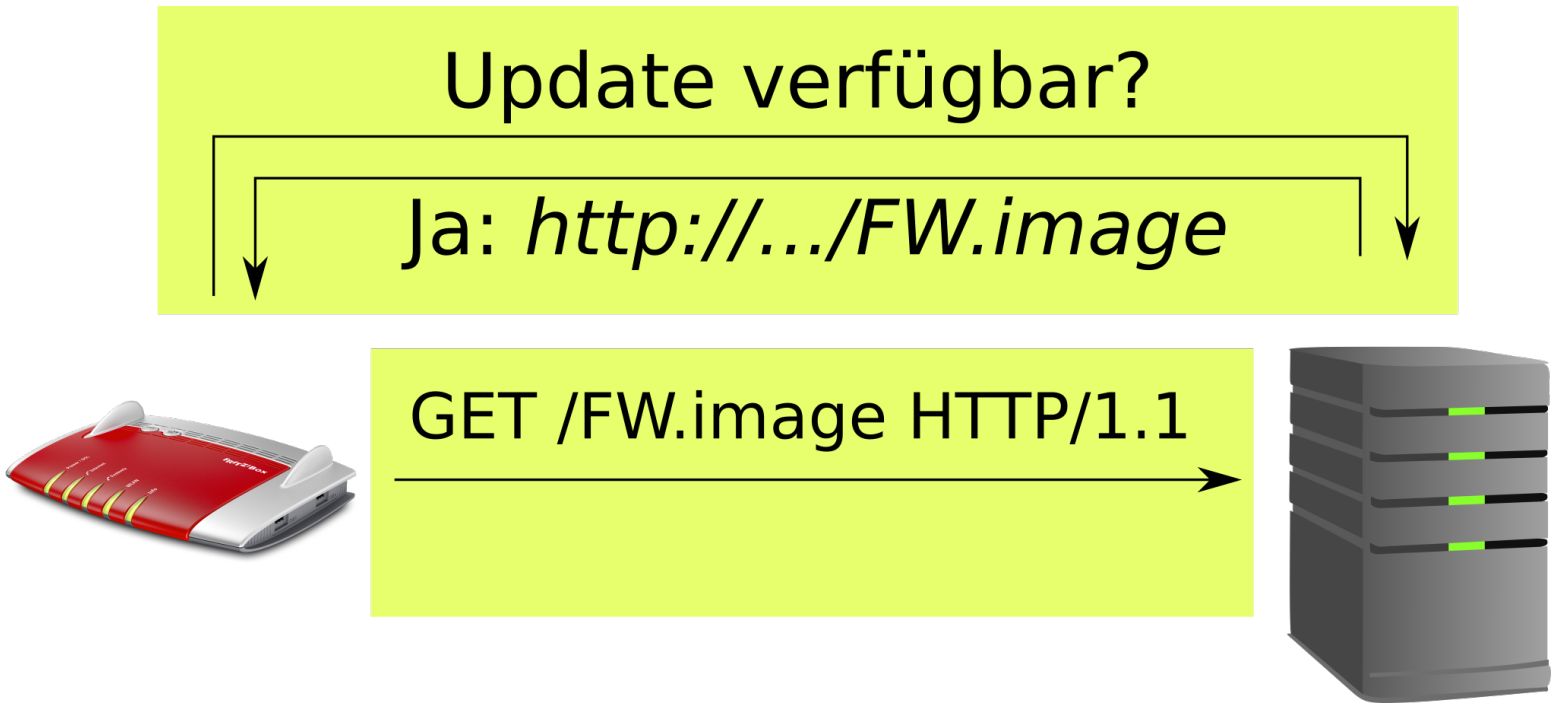
Reguläre Übertragung von Firmware-Updates



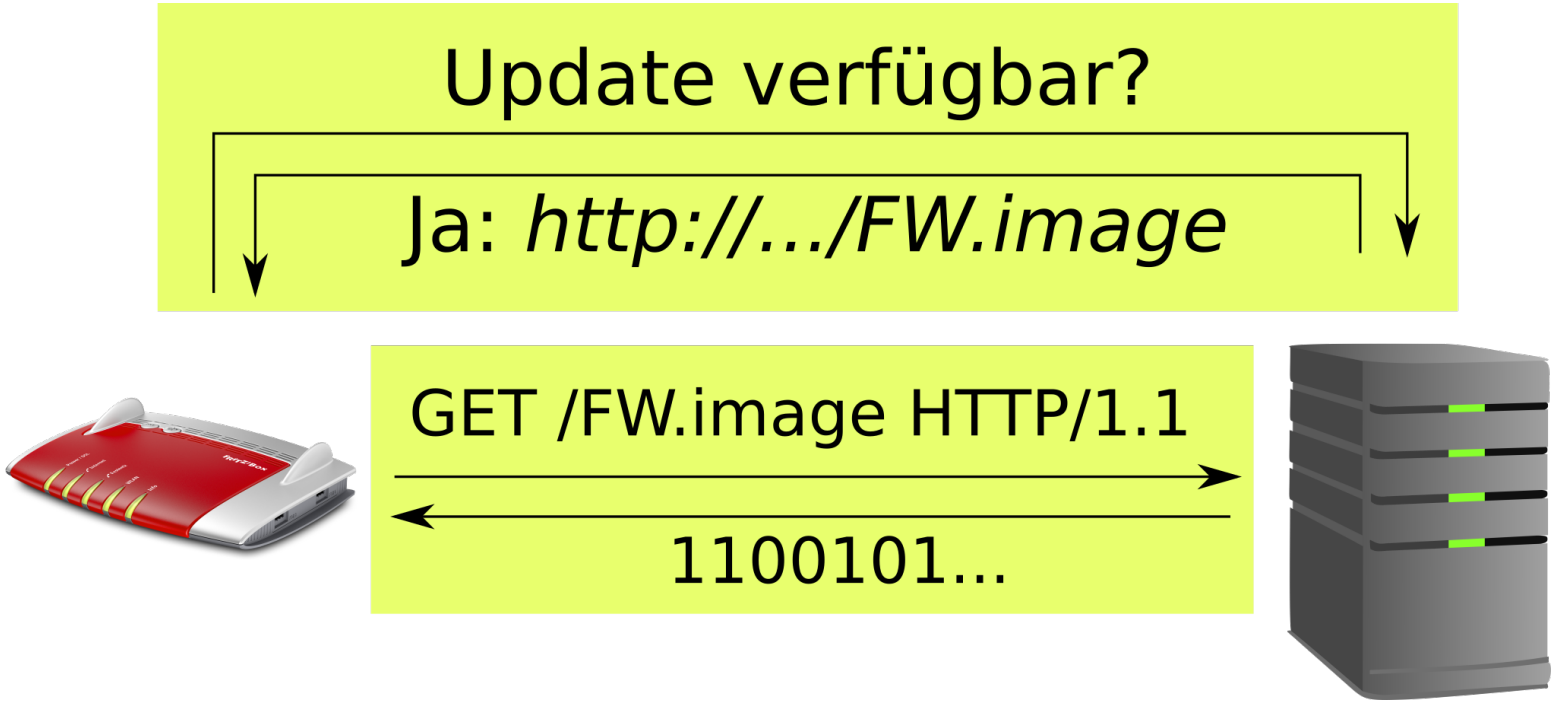
Reguläre Übertragung von Firmware-Updates



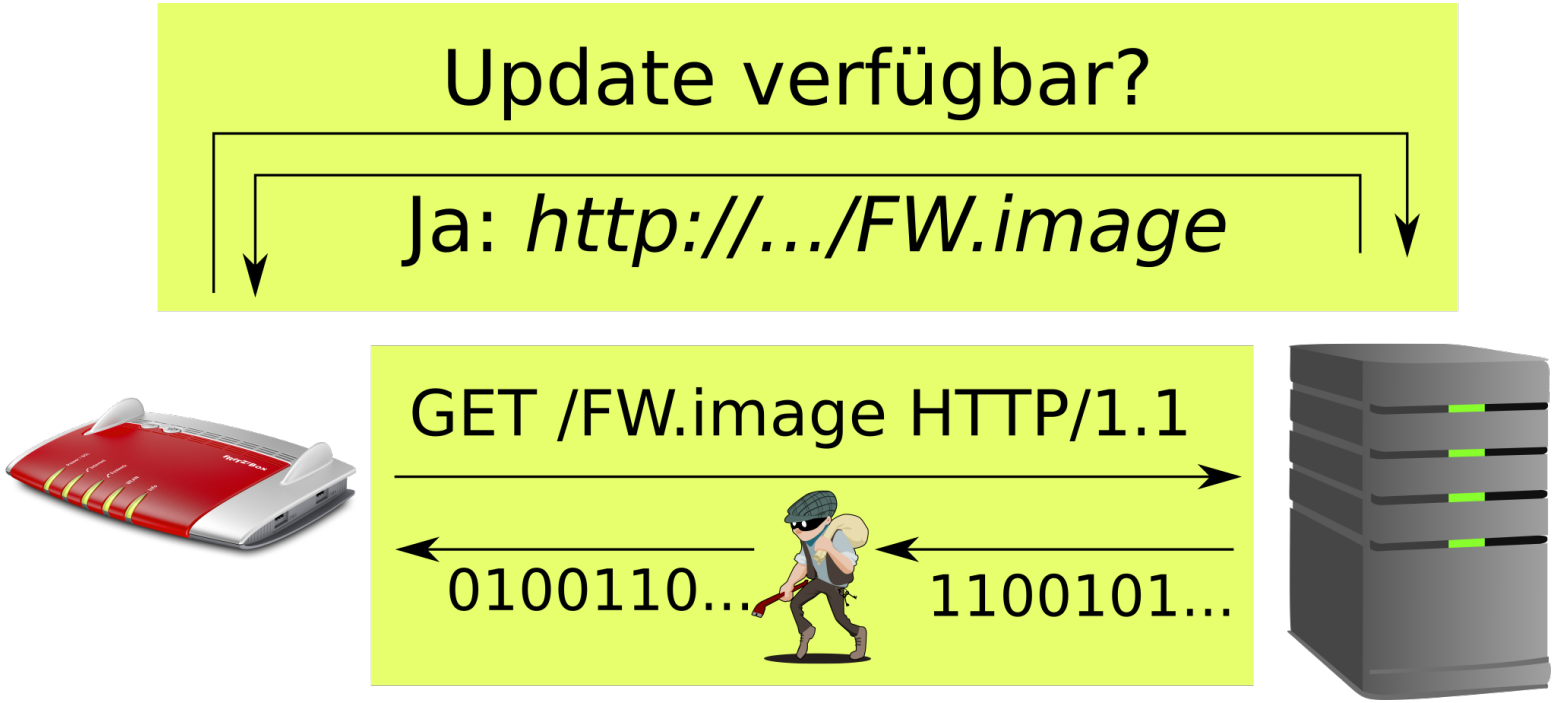
Reguläre Übertragung von Firmware-Updates



Reguläre Übertragung von Firmware-Updates



Manipulierte Übertragung von Firmware-Updates



Tar-Archive als Container

```
$ tar --list --file FRITZ.Box_7490.113.06.24.image
./var/
./var/install
./var/chksum
./var/info.txt
./var/tmp/
./var/tmp/filesystem.image
./var/tmp/kernel.image
./var/regelex
./var/signature
```

Tar-Archive als Container

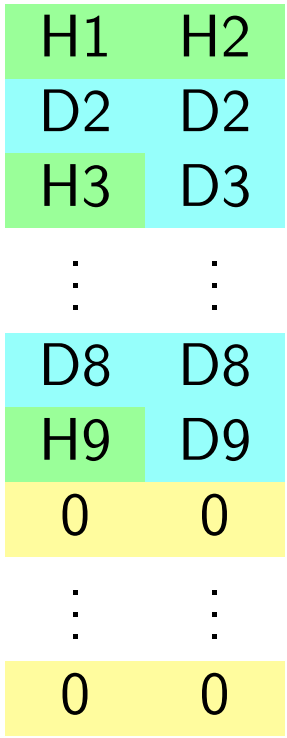
```
$ tar --list --file FRITZ.Box_7490.113.06.24.image
./var/
./var/install
./var/chksum
./var/info.txt
./var/tmp/
./var/tmp/filesystem.image
./var/tmp/kernel.image
./var/regelex
./var/signature
```

← Shell-Skript wird nach erfolgreicher Verifizierung aufgerufen

← Signatur zur Verifizierung des Firmware-Images

Tar-Archive als Container

```
$ tar --list --file FRITZ.Box_7490.113.06.24.image
./var/
./var/install
./var/chksum
./var/info.txt
./var/tmp/
./var/tmp/filesystem.image
./var/tmp/kernel.image
./var/regelex
./var/signature
```



Erstellen der Signatur

Nachricht `A`

H1	H2
D2	D2
H3	D3
⋮	⋮
D8	D8
H9	D9
0	0
⋮	⋮
0	0

- ★ Signatur (`H9`, `D9`) kann nicht von sich selbst abhängen

Erstellen der Signatur

Nachricht `A`

H1	H2
D2	D2
H3	D3
⋮	⋮
D8	D8
H9	D9
0	0
⋮	⋮
0	0

Nachricht `B`

H1	H2
D2	D2
H3	D3
⋮	⋮
D8	D8
0	0
0	0
⋮	⋮
0	0

- ★ Signatur (`H9`, `D9`) kann nicht von sich selbst abhängen
- ★ 1024 Nullbytes als Platzhalter (rot)

Erstellen der Signatur

Nachricht `A`

H1	H2
D2	D2
H3	D3
⋮	⋮
D8	D8
H9	D9
0	0
⋮	⋮
0	0

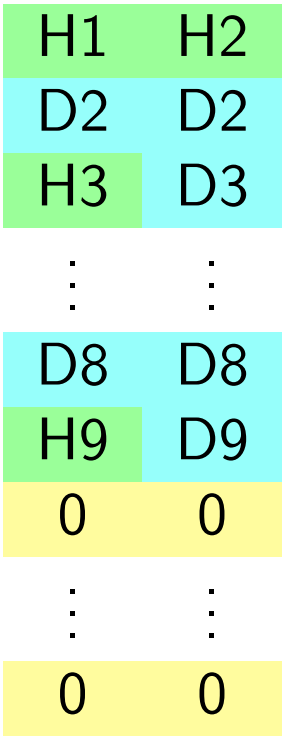
Nachricht `B`

H1	H2
D2	D2
H3	D3
⋮	⋮
D8	D8
0	0
0	0
⋮	⋮
0	0

- ★ Signatur (`H9`, `D9`) kann nicht von sich selbst abhängen
- ★ 1024 Nullbytes als Platzhalter (rot)
- ★ AVM signiert Nachricht `B` und ersetzt den Platzhalter durch die Signatur

Überprüfen der Signatur

Nachricht `A`



- ★ Suche enthaltene Signatur
- ★ Ersetze vorübergehend durch Nullbytes
- ★ Prüfe Signatur

Überprüfen der Signatur

Nachricht `A`

H1	H2
D2	D2
H3	D3
⋮	⋮
D8	D8
H9	D9
0	0
⋮	⋮
0	0

- ★ Suche enthaltene Signatur
- ★ Ersetze vorübergehend durch Nullbytes
- ★ Prüfe Signatur

```
if (strstr(filename, "/var/signature"))
{
  // Signatur an Position x gefunden
  // Ersetze Hx/Dx durch Nullbytes
}
```

Neue Datei einfügen

Können wir eine weitere Datei in das Tar-Archiv einfügen, ohne die Signatur zu beeinflussen?

Neue Datei einfügen

Nachricht `A`

(a)	→	H1	H2
		D2	D2
		H3	D3
		⋮	⋮
		D8	D8
(b)	→	H9	D9
(c)	→	0	0
		⋮	⋮
(d)	→	0	0

Welche Position würde ein Angreifer wählen?

Neue Datei einfügen

Nachricht `A`

(a)	→	H1	H2
		D2	D2
		H3	D3
		⋮	⋮
		D8	D8
(b)	→	H9	D9
(c)	→	0	0
		⋮	⋮
(d)	→	0	0

Welche Position würde ein Angreifer wählen?

	Signatur	Tar
(a)	X	ok
(b)	X	ok
(c)	ok	ok
(d)	ok	X

⇒ Möglichkeit (c) vielversprechend

Name der neuen Datei

```
if (strstr(filename, "/var/signature"))
```

```
    /var/signature
(e) ./var/signature
    ./tmp/var/signature/example
(f) ./var/signature/../../var/install
(g) ./var/install/../../var/signature
```

- ★ Alle Beispiele werden wie Signaturdateien behandelt
- ★ Welcher Dateiname hilft einem Angreifer?

Name der neuen Datei

```
if (strstr(filename, "/var/signature"))
```

```
    /var/signature
(e) ./var/signature
    ./tmp/var/signature/example
(f) ./var/signature/../../var/install
(g) ./var/install/../../var/signature
```

- ★ Alle Beispiele werden wie Signaturdateien behandelt
- ★ Welcher Dateiname hilft einem Angreifer?

Verhalten von Tar

```
$ tar xf FRITZ.Box_7490.113.06.24.image 2>/dev/null
./var/
./var/install
[...]
./var/tmp/kernel.image
./var/regelex
./var/signature
./var/signature/../../var/install
```

- ★ Zielpfad der Datei?

Verhalten von Tar

```
$ tar xf FRITZ.Box_7490.113.06.24.image
./var/
./var/install
[...]
./var/tmp/kernel.image
./var/regelex
./var/signature
tar: Removing leading ‘/var/signature/../’ from
     member names
./var/signature/../../var/install
```

- ./var/install wird überschrieben

Zusammenfassung

- ★ Beliebige Befehle auf der FRITZ!Box ausführbar
- ★ Persistenter Zugriff auf Internetverbindung und Heimnetzwerk (Network Attached Storage, VoIP-Telefone, Drucker, . . .)
- ★ Ausnutzbar für Man-in-the-Middle-Angreifer (Netzbetreiber, Geheimdienste, . . .)
- ★ Von AVM korrigiert seit Mitte 2014

Zusammenfassung

- ★ Beliebige Befehle auf der FRITZ!Box ausführbar
- ★ Persistenter Zugriff auf Internetverbindung und Heimnetzwerk (Network Attached Storage, VoIP-Telefone, Drucker, . . .)
- ★ Ausnutzbar für Man-in-the-Middle-Angreifer (Netzbetreiber, Geheimdienste, . . .)
- ★ Von AVM korrigiert seit Mitte 2014

Proof-of-Concept und Advisory:

https://www.redteam-pentesting.de/advisories/rt-sa-2014-010