Sicherheit und Vertrauen

Erfahrungen als Open Source Hacker

Stefan Schumacher

sicherheitsforschung-magdeburg.de
stefan.schumacher@sicherheitsforschung-magdeburg.de

Chemnitzer Linux-Tage 2017

Id: FLOSS-Hacker-Input.tex,v 1.4 2017/02/24 17:55:23 stefan Exp



Über Mich



Über Mich

- Bildungswissenschaft/Psychologie
- Geek, Nerd, Hacker seit mehr als 20 Jahren
- einige Zeit NetBSD-Entwickler
- Berater für Finanzinstitute, Regierungen, Sicherheitsbehörden
- Direktor des Magdeburger Instituts für Sicherheitsforschung
  Forschungsprogramme zur Unternehmenssicherheit
- Herausgeber des Magdeburger Journals zur Sicherheitsforschung
- `www.Sicherheitsforschung-Magdeburg.de`



Forschungsprogramme des MIS

- Psychologie der Sicherheit
  - Social Engineering
  - Security Awareness, Sicherheit in Organisationen
  - Didaktik der Sicherheit
  - Didaktik der Kryptographie
- Lehrerfortbildung
  - Lernfelder: Fachinformatiker IT-Sicherheit
  - Lernfelder: IT-Sicherheit für Kaufleute
  - Lernfelder: IT-Sicherheit für Elektroberufe
- IT-Sicherheit in KMU
  - empirische Grundlagenforschung
  - didaktische Aufbereitung
  - Schulungen

Kooperationspartner gesucht!

Inhaltsverzeichnis

1 Intro

2 Vertrauen?

3 Komplexität

4 Psychologie



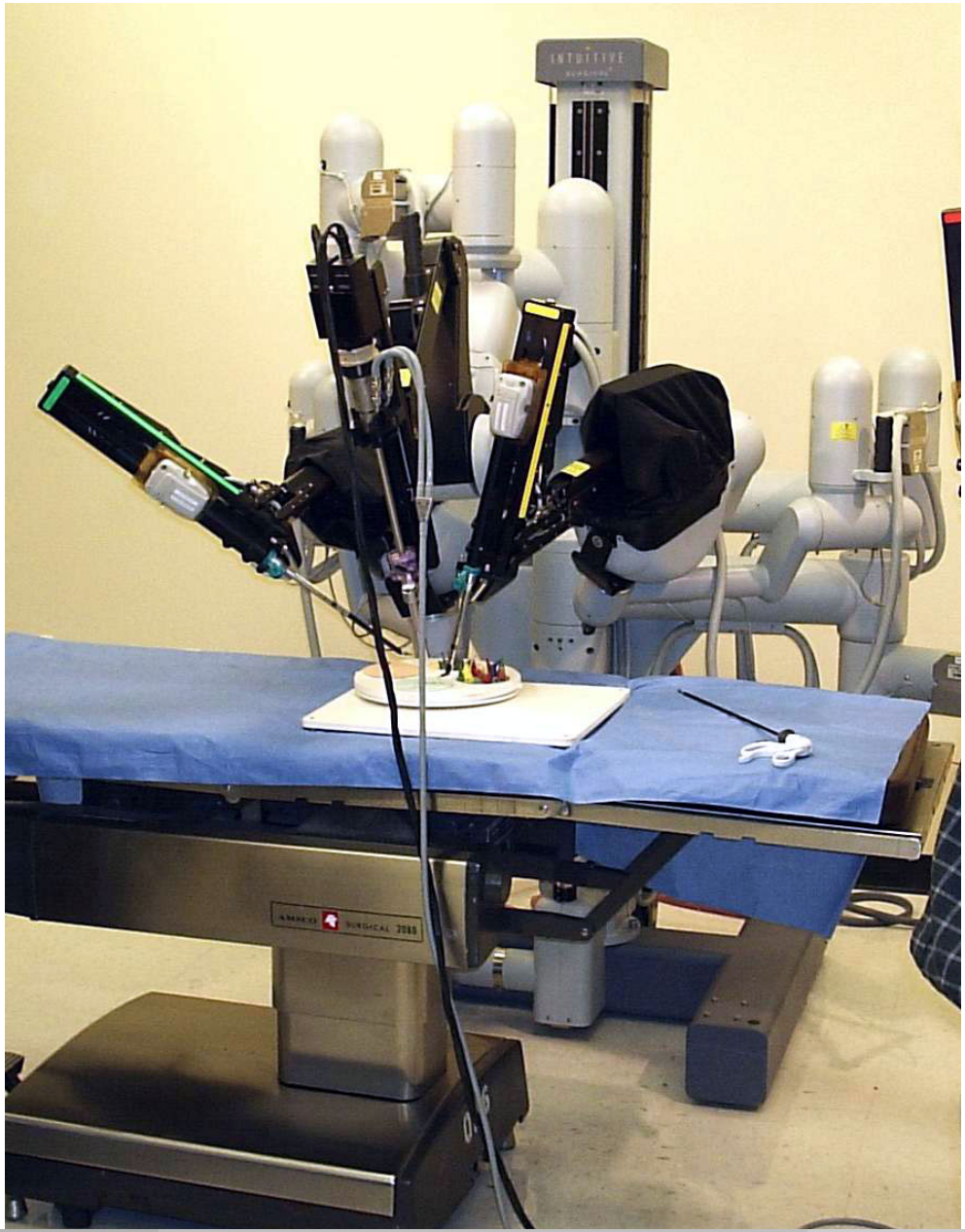
Definition (Outrage as a Svc @OaaSvc)

Science is awesome. You aren't doing science in infosec. Why not? Seems to be the overriding message of @0xKaishakunin #AusCERT2014

- 2013 DeepSec Wien: Psychology of Security - a Research Programme
- 2014 AusCERT Australien: Security in a Post NSA age
- 2015 PHDays Moskau: Why IT Security is fucked up
- 2015 Austrian Trust Circle: Vertrauen ist gut, Kontrolle unmöglich



Chirurgischer Roboter



LEFT-PAD/INDEX.JS

```
module.exports = leftpad;
function leftpad (str, len, ch) {
  str = String(str);
  var i = -1;
  if (!ch && ch !== 0) ch = ' ';
  len = len - str.length;
  while (++i < len) {
    str = ch + str;
  }
  return str;
}
```



Zukunft?

- massive Abhängigkeit von IT
- massive Kenntnislosigkeit von IT-Sicherheit
- insbesondere in der Informatik
- schlechte/fehlende Ausbildung
- keine wissenschaftliche Absicherung/Fundierung
- $\rightsquigarrow$ Psychologie der Sicherheit



Psychologie?

Definition (Psychologie)

Psychologie ist eine empirische Wissenschaft. Sie beschreibt und erklärt das **Erleben und Verhalten des Menschen**, seine Entwicklung im Laufe des Lebens und alle dafür maßgeblichen inneren und äußeren Ursachen und Bedingungen.

Definition (Empirie)

Unter Empirie wird in der Wissenschaft eine im Labor oder im Feld durchgeführte Sammlung (oft Erhebung) von Informationen verstanden, die auf gezielten, systematisch verlaufenden Untersuchungen beruht.

Warum Psychologie der Sicherheit?

- Sicherheit als ein Sonderfall von Lebenswirklichkeit
- Ist ein Gerät oder eine Situation sicher?
- Windows $\prec$ Mac OS X $\prec$ Gentoo Linux $\prec$ OpenBSD
- Sicherheit in der Psychologie: bspw. F20.0 paranoide Schizophrenie
- Fight-or-Flight Reaction (limbisches System)
- Maslowsche Pyramide



Bsp: Buffer Overflow

- Zu große Daten werden in einen zu kleinen Buffer geschrieben
- Buffer-Grenzen laufen über, Speicher-Sicherheit wird verletzt
- Mögliche Konsequenz: Return-Adresse einer Sub-Routine wird mit beliebigen Daten überschrieben $\rightsquigarrow$ Root-Rechte
- Programmierer muss »nur« passende Befehle verwenden . . .



Bsp: Buffer Overflow

- Zu große Daten werden in einen zu kleinen Buffer geschrieben
- Buffer-Grenzen laufen über, Speicher-Sicherheit wird verletzt
- Mögliche Konsequenz: Return-Adresse einer Sub-Routine wird mit beliebigen Daten überschrieben $\rightsquigarrow$ Root-Rechte
- Programmierer muss »nur« passende Befehle verwenden …



Buffer Overflow in C

Das Problem

```
1 void input_line()
2 {    char line[1000];
3      if (gets(line))
4          parse_line(line);
5 }
```

`line` mit Länge 1000 deklariert
`gets` zeigt auf Array *ohne Länge*
wenn `line` größer 1000 = Problem
Thou shalt not follow the pointer



Buffer Overflow in C

Die Lösung

```
1 void input_line()
2 {    char line[1000];
3      if (fgets(line, sizeof(line), stdin))
4          parse_line(line);
5 }
```

`gets` zeigt auf Array *mit Länge*

Hardwarenahe Sprachen meiden, Compiler mit Feldüberwachung, PaX, `w^x` ...

Problem: Mensch muss entscheiden!



Eine kurze Geschichte des Buffer Overflows

- 02.11.1988: Morris-Wurm nutzte u. a. einen Buffer-Overflow via `gets()` in finger(1)
- 1996: Aleph One *Smashing the Stack for Fun and Profit* in Phrack 49
- 2001: Code Red
- 2008: SQL Slammer
- CORE-2007-0219: OpenBSD's IPv6 mbufs remote kernel buffer overflow
- 2007: Buffer Overflow in Snort
- VU#987308: HP LoadRunner buffer overflow vulnerability



1996: Ariane 5 Flight 501



Ariane 5 Flug 501

- 1996 Ariane 5 501: gesprengt nach 36,7 Sekunden
- Software von Ariane 4 auf Ariane 5 portiert
- 64 Bit Float in 16 Bit signed Int
- Beschleunigung der Ariane 5 ist signifikant höher $\rightsquigarrow$ Overflow
- Test-Simulation vor dem Flug fand das Problem nicht, Nicht-Schutz der Variablen war nicht dokumentiert
- 320 000 000,– Euro teures Feuerwerk



Inhaltsverzeichnis

1 Intro

2 Vertrauen?

3 Komplexität

4 Psychologie



Vertrauen?

- Open Source ist sicher!!Eintausendeinhundertelf!!
- Reflections on Trusting Trust
- Vertrauen ist gut, Kontrolle ist besser? Oder unmöglich?
- Was ist Vertrauen?
- Was Komplexität?
- Was ist Sicherheit überhaupt?
- Wie kann ich Sicherheit messen?
- Wie Sicherheit generieren?
- Psychologie der Sicherheit



Vertrauen?

- Open Source ist sicher!!Eintausendeinhundertelf!!
- Reflections on Trusting Trust
- Vertrauen ist gut, Kontrolle ist besser? Oder unmöglich?
- Was ist Vertrauen?
- Was Komplexität?
- Was ist Sicherheit überhaupt?
- Wie kann ich Sicherheit messen?
- Wie Sicherheit generieren?
- Psychologie der Sicherheit



Vertrauen

Ist Kontrolle möglich?

- Reflections on Trusting Trust
- 1984, Turing Award Speech, basiert auf
- Karger, Paul A.; Schell, Roger R. (June 1974). Multics Security Evaluation: Vulnerability Analysis
- Compiler wird manipuliert
- baut Backdoor in kompilierten Code ein
- Compiler kompiliert Backdoor in kompilierten Compiler ein ...



Vertrauen

Ist Kontrolle möglich?

- Verifikation technischer Systeme theoretisch möglich
- IT-Systeme sind zu komplex um wirklich überprüft zu werden
- NetBSD:ca. 163 000 Quelldateien, 57 228 442 LoC, 1 991 091 842 Zeichen
- Faust I: 4 600 Zeilen, 200 000 Zeichen
- der Verteidiger muss *alle* Systeme erfolgreich verteidigen, der Angreifer nur *eine einzige* Sicherheitslücke ausnutzen



Vertrauen

Ist Kontrolle möglich?

Ist GnuPG sicher?

1. GnuPG-Implementierung?
2. mutt?
3. vim?
4. Userland?
5. OS-Kernel?
6. Treiber-Blobs?
7. BIOS/UEFI?
8. Festplatte?
9. AES? SHA1?
10. Mathematik?
11. Gödel?



Vertrauen

laut Luhmann

- ein Mittel zur Reduktion sozialer Komplexität
- muss *immer* gewährt werden
- komplexere Umwelt erzwingt funktional ausdifferenzierte Systeme
- z.B. Medizin, Recht, Politik, Medien, Hacker, IT-Experten ...



Vertrauen

laut Luhmann

- Subsysteme müssen miteinander kommunizieren, Schnittstellen entstehen
- jeder Experte kann nicht alles wissen, da nicht die gesamte Umwelt aufgenommen werden kann
- d.h. Experten müssen zusammen arbeiten und einander vertrauen
- dazu haben sich Diagnosekriterien entwickelt
  z.B. formale Bildungsabschlüsse in D, Empfehlungsschreiben in USA, Familienbeziehungen in Saudi-Arabien
- Komplexität wird damit reduziert, Vertrauen gewährt
- Vertrauen an die Entwickler etc. von FLOSS



Inhaltsverzeichnis

1 Intro

2 Vertrauen?

3 Komplexität

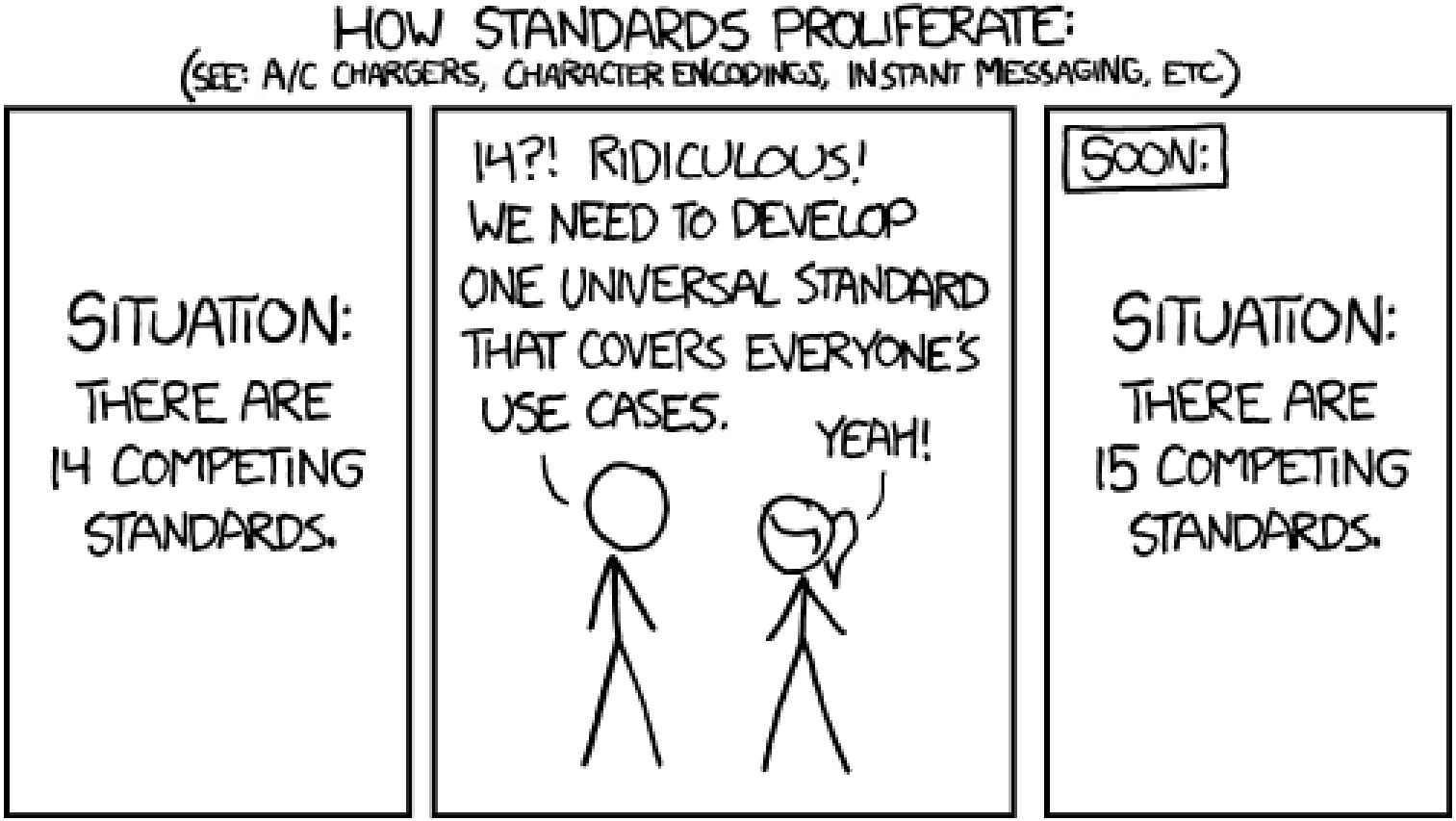
4 Psychologie



- Komplexitätstheorie der theoretischen Informatik
- maximaler Ressourcenbedarf eines Algorithmus
- idR Zeitkomplexität oder Platzkomplexität
- Landau-Symbol/Groß-O
  - Bubblesort: $\mathcal{O}(n^2)$
  - Mergesort: $\mathcal{O}(n \cdot \log(n))$
  - Bogosort: $\mathcal{O}(n \cdot n!)$
  - Slowsort: $\mathcal{O}\left(n^{\frac{\log(n)}{(2+e)}}\right)$



- soziale Komplexitätsreduktion gibt es nicht
- Standards sind etwas feines, jeder sollte einen haben ...



Komplexitätsreduktion

Soziologie

- OpenSSL Heartbleed
- OpenBSD forks, prunes, fixes OpenSSL $\rightsquigarrow$ LibreSSL
- Diskussion entsteht: Warum kein Komitee, dass die OpenSSL-Entwicklung steuert?
- Grundgesetz der Steuerungstechnik: Das steuernde System ist immer mindestens genau so komplex wie das zu steuernde System
- jedes neue Steuerelement führt weitere Komplexität ein
- und erhöht damit u.a. die Angreifbarkeit



Inhaltsverzeichnis

1 Intro

2 Vertrauen?

3 Komplexität

4 Psychologie



GEFÜHLTE SICHERHEIT ERFORSCHEN

- Kernaufgabe der Psychologie, Pädagogik, Soziologie, Politikwissenschaft
- empirischen Sozialforschung: quantitative und qualitative
- quantitativ: alle Vorgehensweisen zur numerischen Darstellung empirischer Sachverhalte
- qualitativ: Erhebung nicht standardisierter Daten und deren Auswertung; interpretative und hermeneutische Methoden als Analysemittel

Persönlichkeitseigenschaften und Sicherheit

- Neurotizismus
- Extraversion
- Offenheit für Erfahrungen
- Verträglichkeit
- Gewissenhaftigkeit

Wie beeinflussen diese Persönlichkeitseigenschaften die Wahrnehmung von Sicherheit?

Hacker als Forschungsobjekt

- Persönlichkeitseigenschaften von Hackern? Neurotizismus? Offenheit?
- Wie erlernt man Hacker sein? White Hat/Black Hat $\rightsquigarrow$ Biographisierung
- Lernen en passant, informelles Lernen, formales Lernen, selbstgesteuertes Lernen
- Dipl.-Inf. vs. Hacker - was unterscheidet sie?
- Ausbildung vs. Bildung
- Motive und Motivation



Open Source Communities als Forschungsobjekt

- Kommunikation, Selbstorganisation
- Steering Commitee vs. BDFL
- Erfahrung: smb@NetBSD.org
- Überwachung?
- Rechenschaft?
- Komplexität: NetBSD src.tgz 201 850 Dateien
- der ideale Entwickler: motiviert, kompetent, erfahren



Didaktik der Sicherheit

- Sicherheitskompetentes Verhalten muss erlernt werden!
- Wie unterrichte ich es?
- Welche Inhalte?
- Welche Methoden?
- Welche Organisationsform? Schule, Ausbildung, Uni, VHS ...
- Fachinformatiker, Fachrichtung IT-Sicherheit einführen?
- Welches Curriculum?

Und nun?

- 14:00 V4
- Einen hochsicheren Laptop mit Ubuntu einrichten



- sicherheitsforschung-magdeburg.de
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- sicherheitsforschung-magdeburg.de/publikationen/journal.html



- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- Xing: Stefan Schumacher
- ZRTP: 0xKaishakunin@ostel.co