Sicherheit und Vertrauen

Erfahrungen als Open Source Hacker

Stefan Schumacher

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

Bitkom Forum Open Source
05.07.2016

Id: FLOSS-Hacker-Input.tex,v 1.3 2016/07/04 12:53:43 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

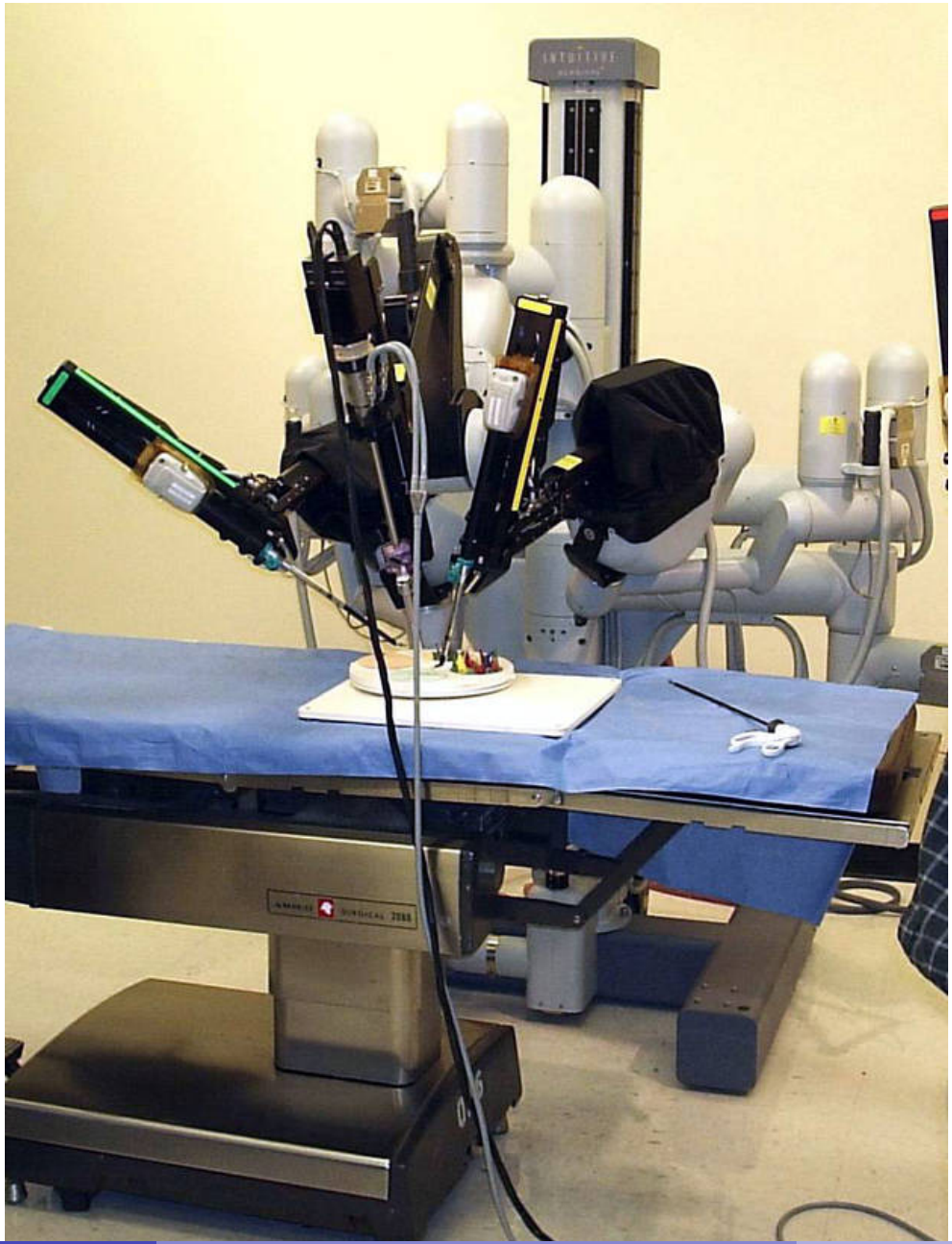
Kooperationspartner gesucht!

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



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 …

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

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?

- 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