The Time-to compromise

by Andrej Zieger
HAW Hamburg / DFN CERT

The Time-to compromise

by Andrej Zieger
HAW Hamburg / DFN CERT

Security by Design...

Guides Bestpractices And More

A lot effort to get IoT secure!

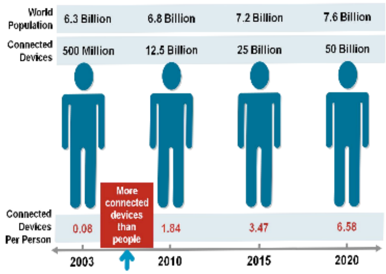
BUILDITSECURE.LY

a community [...] to make the Internet of Things safer for consumers and businesses

enisa

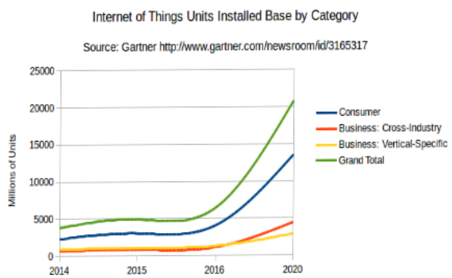
Security and Resilience of Smart Home Environments
Good practices and recommendations

Smart Mass

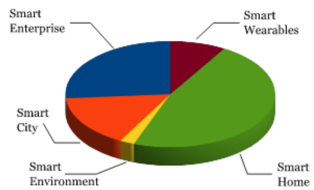


It's more of them than of us

And it is still growing!



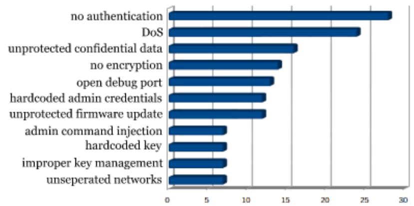
Vulnerabilities Everywhere!



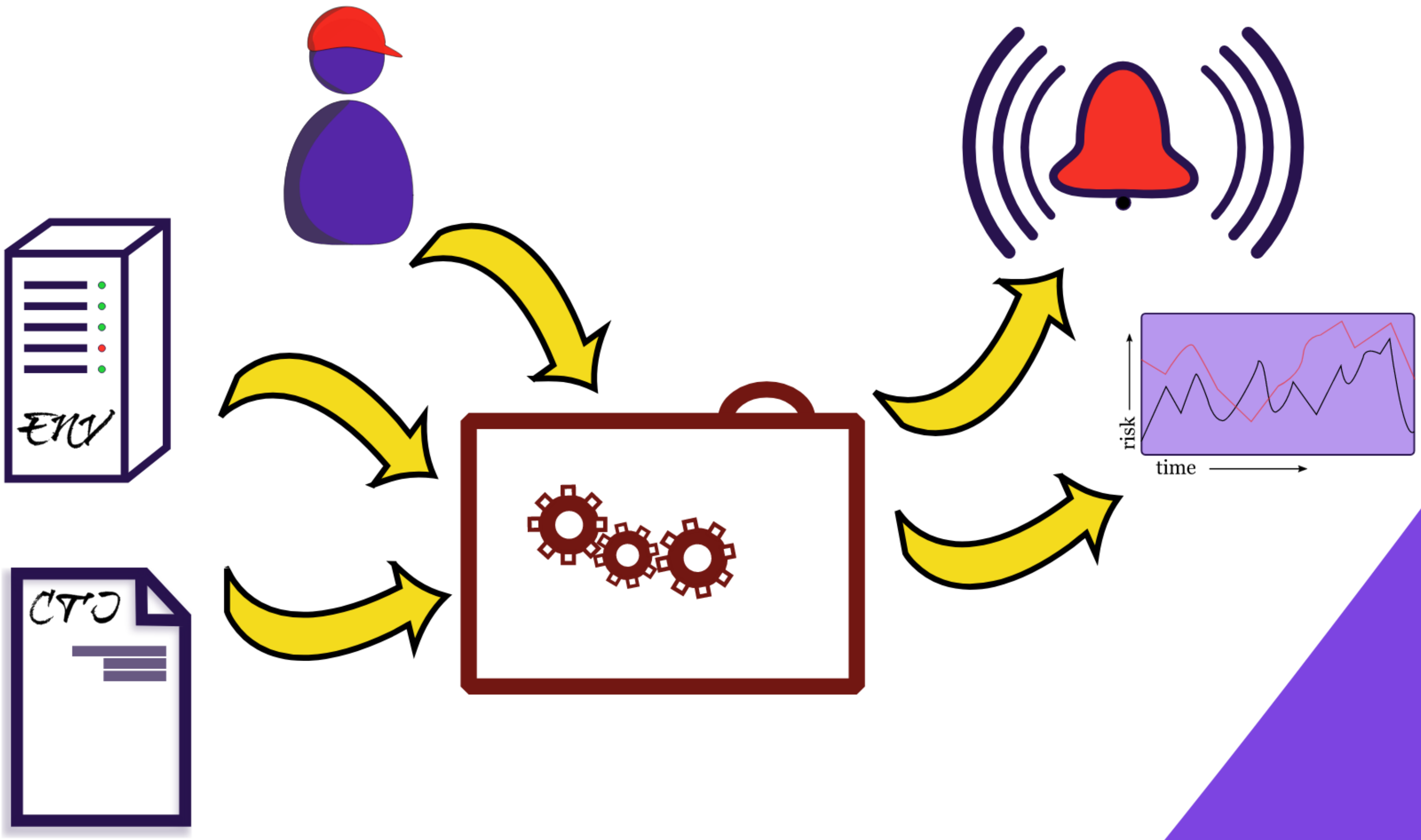
Research public available data
5 Categories
221 Devices considered
119 Vulnerabilities known

Top Vulnerabilities

Count	Type
28	no authentication
24	DoS
16	unprotected confidential data
13	no encryption
12	unprotected firmware update
12	hardcoded admin credentials



How we wanna help



Basic Metric

Time-to-compromise by McQueen

3 stochastic processes

1) exploit ready to go

2) try known vulnerabilities

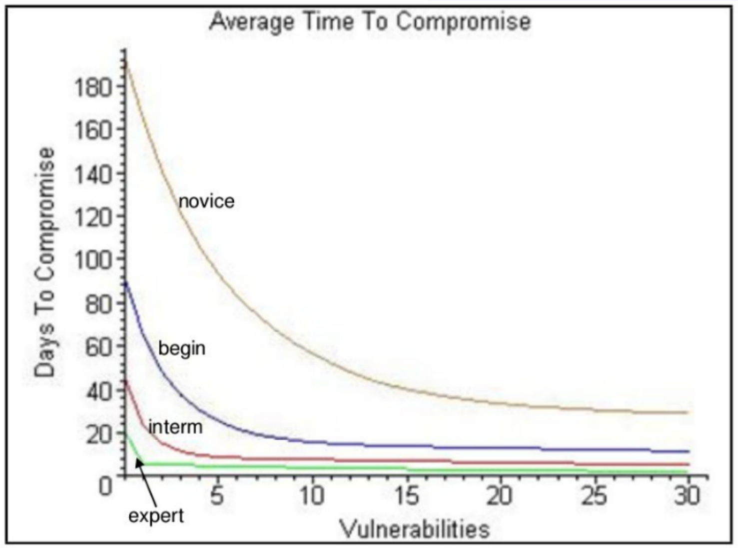
3) search / await zero day

Vuln. count

Skill level

Skill level

$$TTC(v, s, k) = t_1 \cdot P_1 + t_2 \cdot (1 - P_1) \cdot (1 - u) + t_3 \cdot u \cdot (1 - P_1)$$



Basic Metric

Time-to-compromise by McQueen

$$TTC(\overset{\text{Vuln. count}}{v}, \overset{\text{Skill level}}{s}, \overset{\text{Skill level}}{k}) =$$
$$t_1 \cdot P_1 + t_2 \cdot (1 - P_1) \cdot (1 - u) + t_3 \cdot u \cdot (1 - P_1)$$

Basic Metric

Time-to-compromise by McQueen

Vuln. count

Skill level

Skill level

Probability Proc 2 failed

$$u = (1 - f(s))^v$$

time to tune exploit
c1 = 1d

$$TTC(v, s, k) =$$
$$t_1 \cdot P_1 + t_2 \cdot (1 - P_1) \cdot (1 - u) + t_3 \cdot u \cdot (1 - P_1)$$

Probability Proc 1

$$P_1 = 1 - e^{-v \cdot \frac{m(s)}{k}}$$

time to try known vulnerabilities

$$t_2 = c_2 \cdot E(v, s)$$

time to await zero day

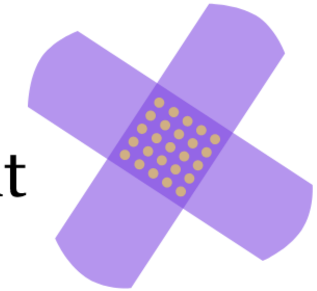
$$t_3 = (\frac{1}{f(s)} - 0.5) \cdot c_3 + c_2$$

Estimated tries

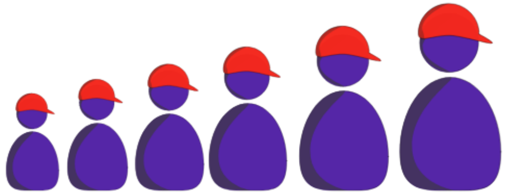
$$E(v, s) = f(s) \cdot \left(1 + \sum_{t=2}^{v - v \cdot f(s) + 1} \left[t \cdot \prod_{i=2}^{t} \left(\frac{v \cdot (1 - f(s)) - i + 2}{v - i + 1}\right)\right]\right)$$

What we will improve

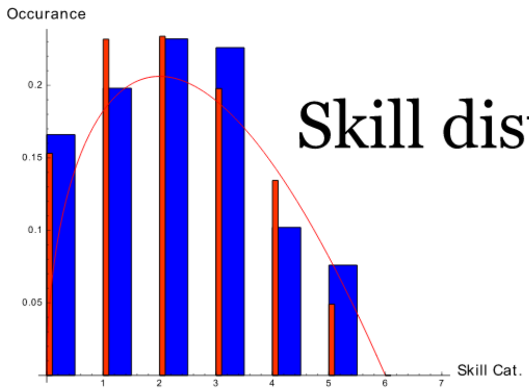
Fix it



Continous skill

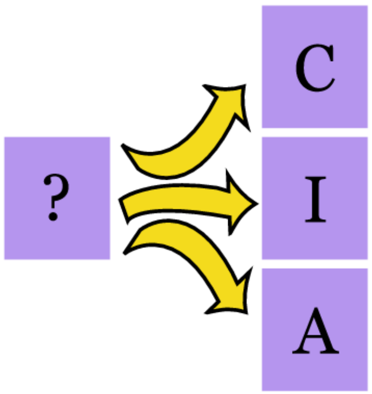


Performance

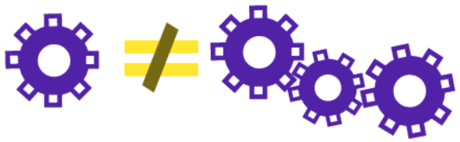


Skill distribution

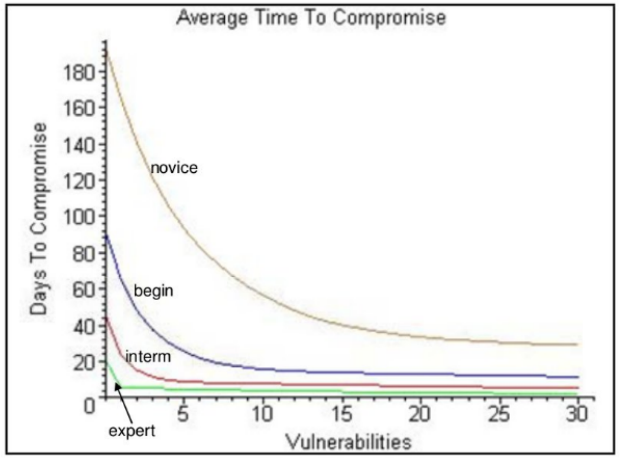
Compromise type

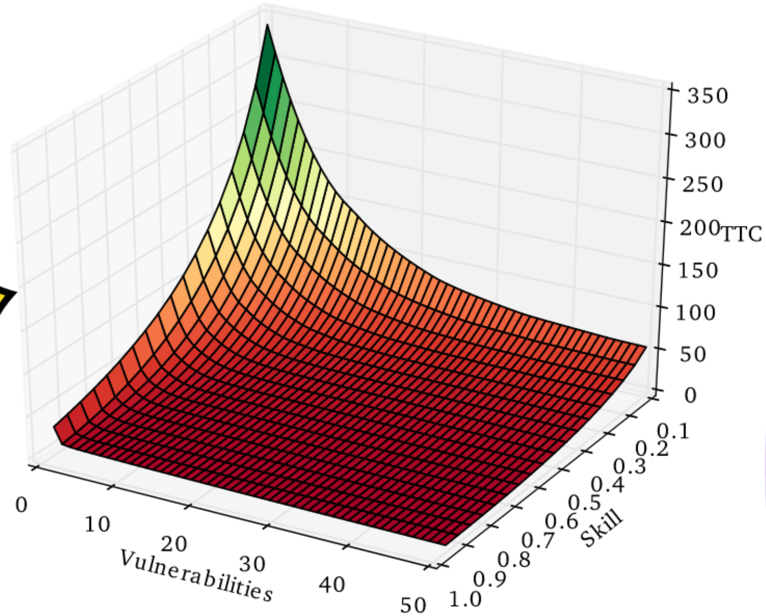


Exploit complexity



Continous Skill





$\mathcal{S} = \{\text{novice, beginner, intermediate, expert}\}$

$TTC : \mathbb{N} \times \mathcal{S} \times \mathbb{N} \rightarrow \mathbb{R}$

$m(s) =$lookup table

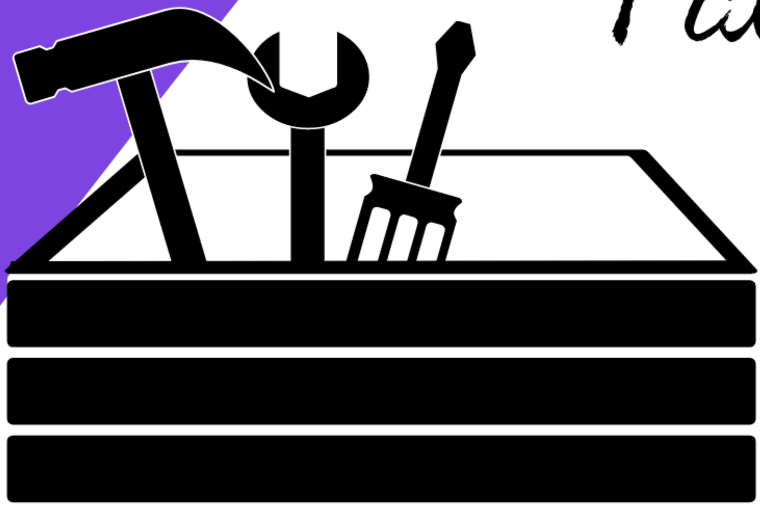
$f(s) =$lookup table

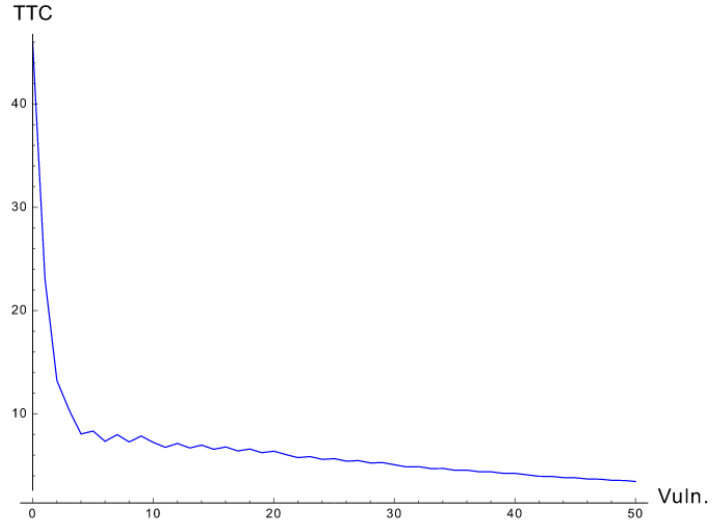
$TTC : \mathbb{N} \times [0,1] \times \mathbb{N} \rightarrow \mathbb{R}$

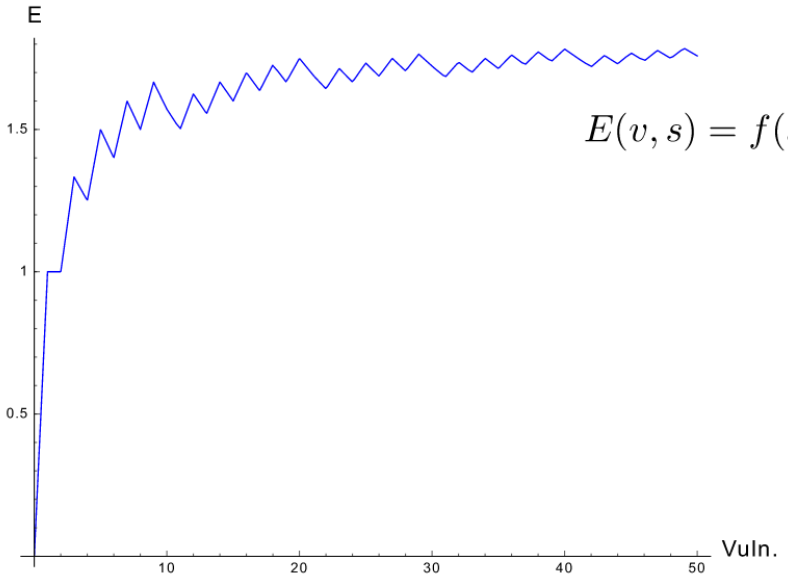
$f(s) = 0.145 \cdot 2.6^{2s+0.07} - 0.1$

$m(s) = 83 \cdot 3.5^{4s/2.7} - 82$

Fix it

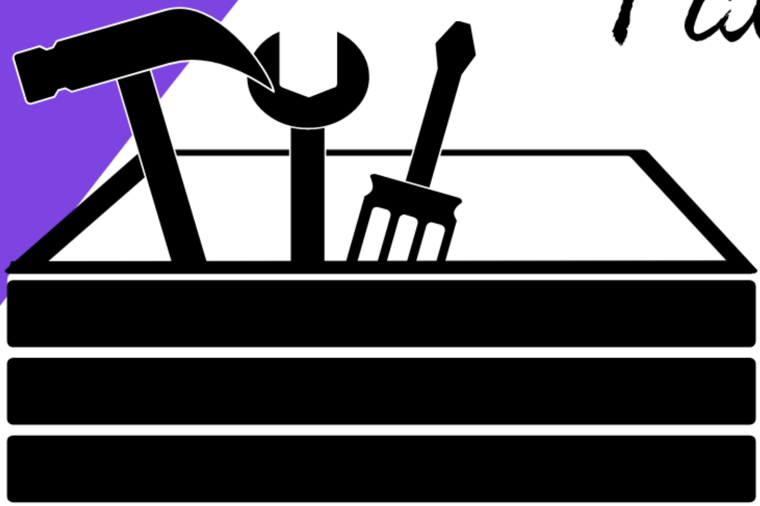


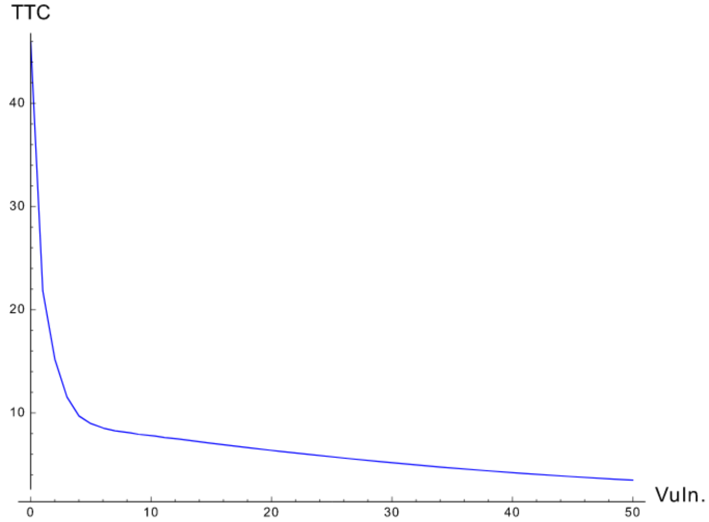


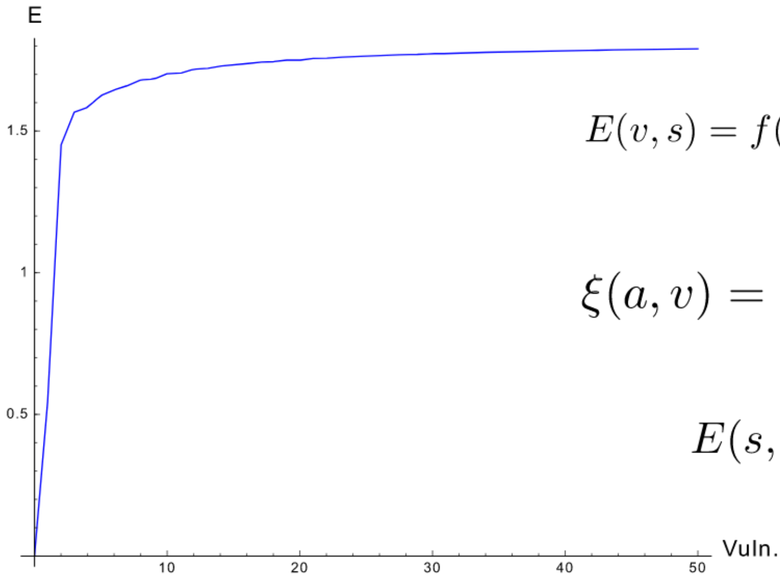


$$E(v,s) = f(s) \cdot \left(1 + \sum_{t=2}^{v - v \cdot f(s) + 1} \left[t \cdot \prod_{i=2}^{t} \left(\frac{v \cdot (1 - f(s)) - i + 2}{v - i + 1} \right) \right] \right)$$

Fix it







$$E(v,s) = f(s) \cdot \left(1 + \sum_{t=2}^{v-v\cdot f(s)+1} \left[t \cdot \prod_{i=2}^{t} \left(\frac{v \cdot (1-f(s)) - i + 2}{v - i + 1} \right) \right] \right)$$

$$\xi(a,v) = \frac{a}{v} \cdot \left(1 + \sum_{t=2}^{\lfloor v\cdot(1-\frac{a}{v})\rfloor+1} \left[t \cdot \prod_{i=2}^{t} \left(\frac{v\cdot(1-\frac{a}{v})-i+2}{v-i+1} \right) \right] \right)$$

$$\begin{aligned} E(s,v) = & \xi(\lfloor f(s)\cdot v \rfloor, v) \cdot (\lceil f(s)\cdot v \rceil - f(s)\cdot v) \\ & + \xi(\lceil f(s)\cdot v \rceil, v) \cdot (1 - \lceil f(s)\cdot v \rceil + f(s)\cdot v) \end{aligned}$$

Performance

$$\xi(a,v) = \frac{a}{v} \cdot \left(1 + \sum_{t=2}^{\lfloor v\cdot(1-\frac{a}{v})\rfloor+1} \left[t \cdot \prod_{i=2}^{t} \left(\frac{v\cdot(1-\frac{a}{v})-i+2}{v-i+1}\right)\right]\right)$$

$$\xi(a,v) = \frac{a}{v} + \frac{a\cdot(v-a)!}{v!} \cdot \sum_{t=2}^{\lfloor v\cdot(1-\frac{a}{v})\rfloor+1} \left[t \cdot \frac{(v-t+1)!}{(v-a-t+1)!\cdot(v-t+1)}\right]$$

Performance Evaluation

TTC0: naive
TTC1 : + continous & fix
TTC2: + using faculty
TTC3: + independent (math complete)
TTC4: + precalculate faculty i < 100

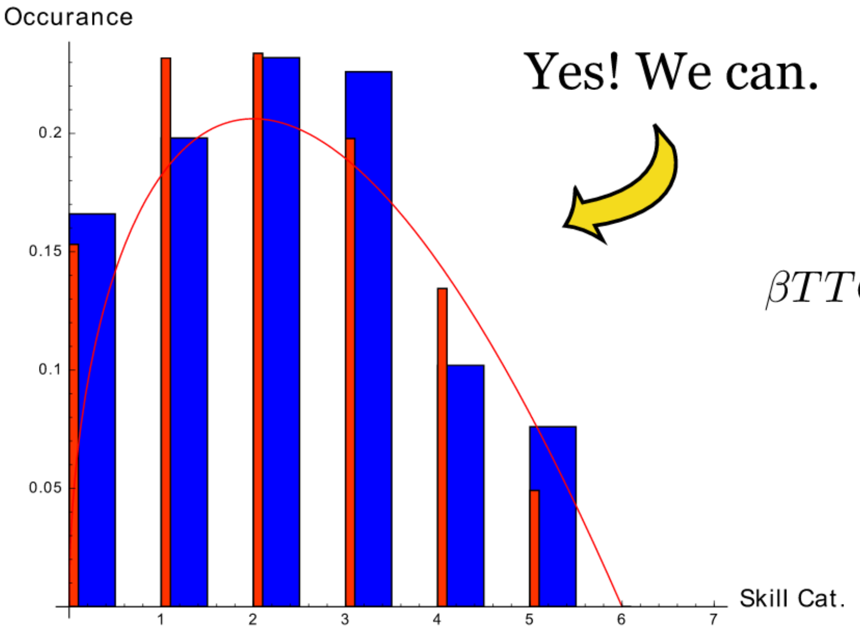
Algorithm	Min	Max	Avg	TTC/sec	Performance
TTC0	13.23s	13.74s	13.37s	150	×1.0
TTC1	8.41s	8.46s	8.44s	237	×1.6
TTC2	1.65s	1.67s	1.66s	1206	×8.1
TTC3	1.06s	1.12s	1.09s	1841	×12.3
TTC4	0.77s	0.80s	0.78s	2552	×17.1

Skill Distribution

Simple idea: skill is a random variable

$$\int_0^1 TTC(v, s, k) \cdot d(s)\,\mathrm{d}s$$

Challange: can we find one in the wild



Yes! We can.

$$d = Beta_{\alpha,\beta},\ \alpha = 1.5 \text{ and } \beta = 2$$

$$\beta TTC_{\alpha,\beta}(v, k) = \int_0^1 TTC(v, s, k) \cdot Beta_{\alpha,\beta}(s)\,\mathrm{d}s$$

Compromise Type

Set of all vulnerabilities

$$\mathcal{V}(\alpha, \tau) = \{y \in \mathcal{W} |\ y \text{ affects } \alpha \text{ for compromise type } \tau\}$$

An asset

Compromise Type

a vulnerability

Types:

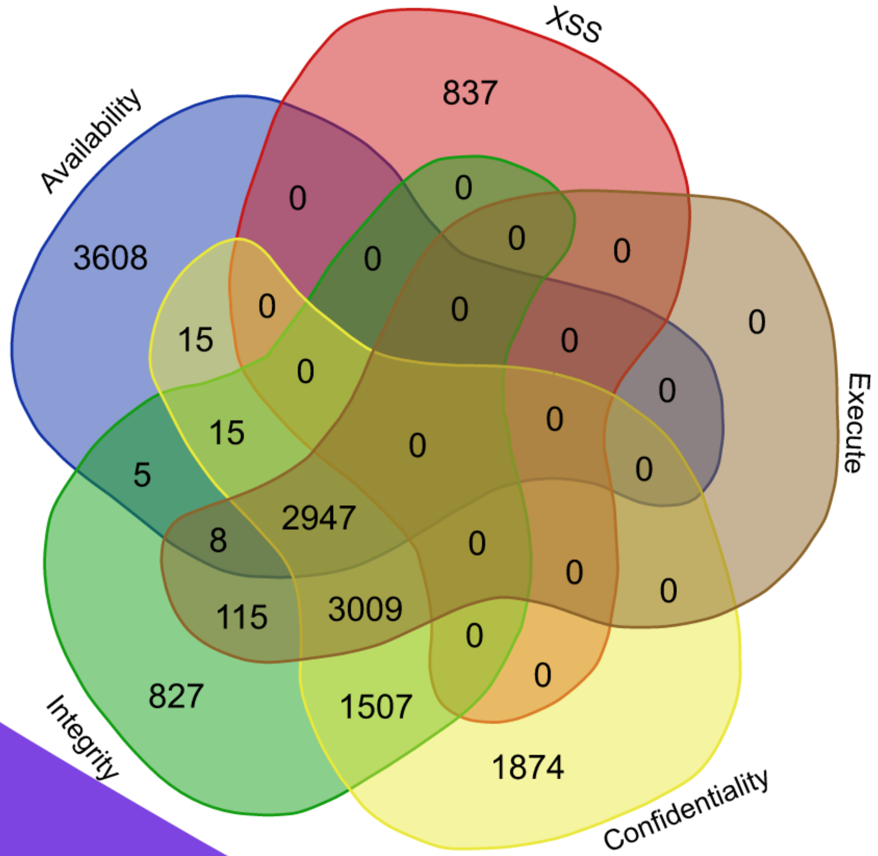
- time-to-compromise-execution (TTCe)
- time-to-compromise-confidentiality (TTCc)
- time-to-compromise-integrity (TTCi)
- time-to-compromise-availability (TTCa)

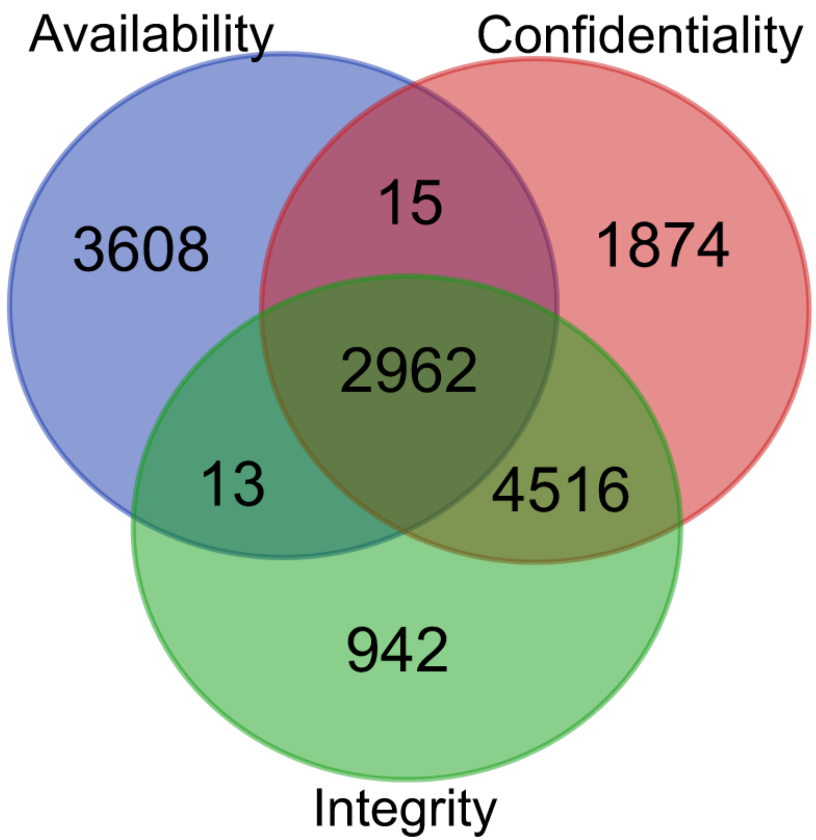
Example TTCa:

$$\begin{aligned}\mathcal{V} = \{y \in \mathcal{W} | y\ & \text{affects } a \text{ and (DAF-effect is DoS} \\ & \text{or CVSS-availability-impact is not none} \\ & \text{or CVSS-integrity-impact is complete)} \\ & \text{and DAF-effect is not XSS}\}\end{aligned}$$

Compromise Type

Evaluation





Exploit Complexity

Exploitability

$$exc(y) = 1 - \left(Ac(y) \cdot Au(y) \cdot \frac{Ex(y) - a_1}{a_2} - a_3 \right) \cdot a_4$$

Constants for scaling

Access complexity

Authentication

Influences:

Probability of having exploit ready

$$P_1 = 1 - e^{-\left(\sum_{y \in \mathcal{V}} 1 - \epsilon \cdot exc(y) \right) \cdot \frac{m(s)}{|W|}}$$

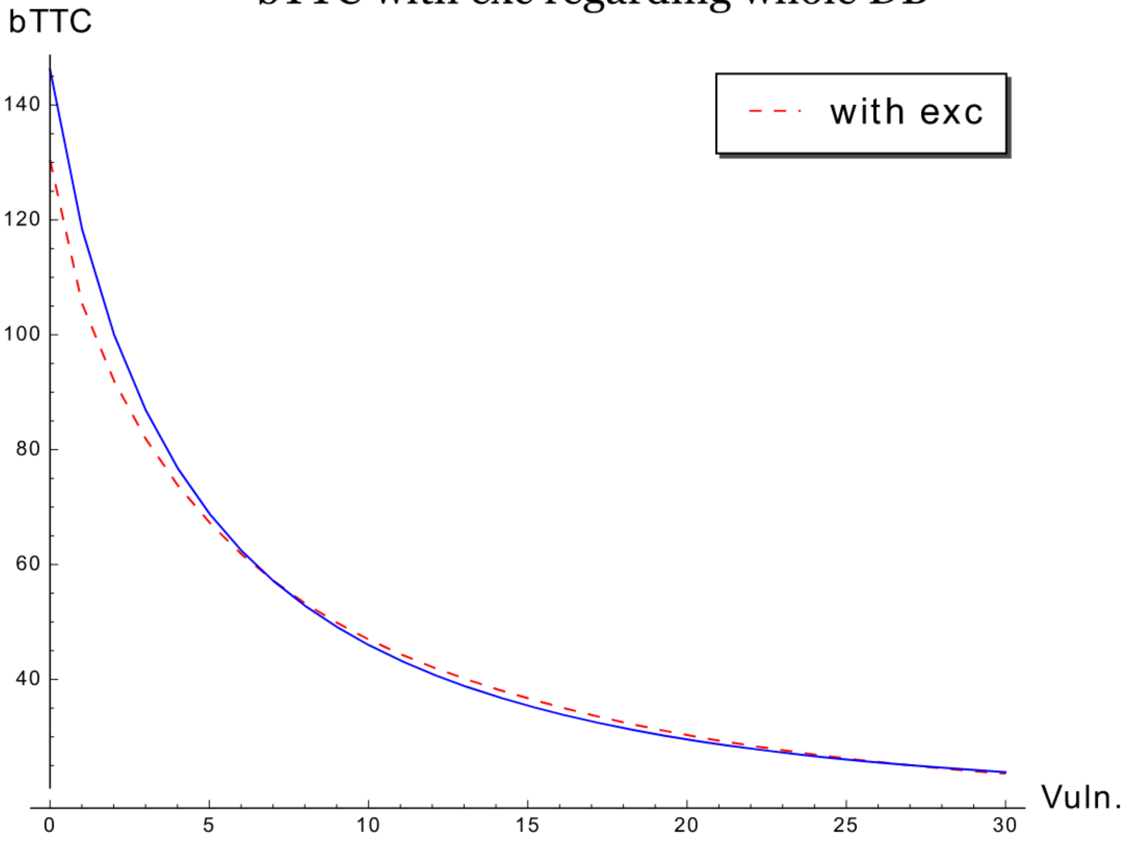
Fraction of usable vulnerabilities

$$f(s) = \left(\frac{|\{y \in W | s > exc(y)\}|}{|W|} + a_5 \right) / a_6$$

Exploit Complexity

Evaluation

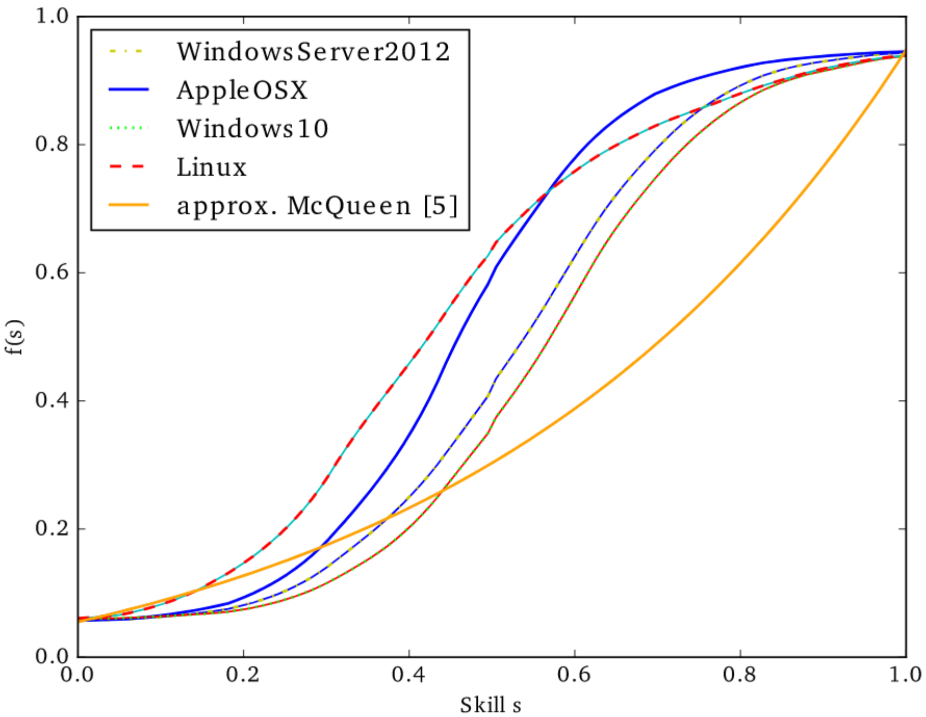
bTTC with exc regarding whole DB

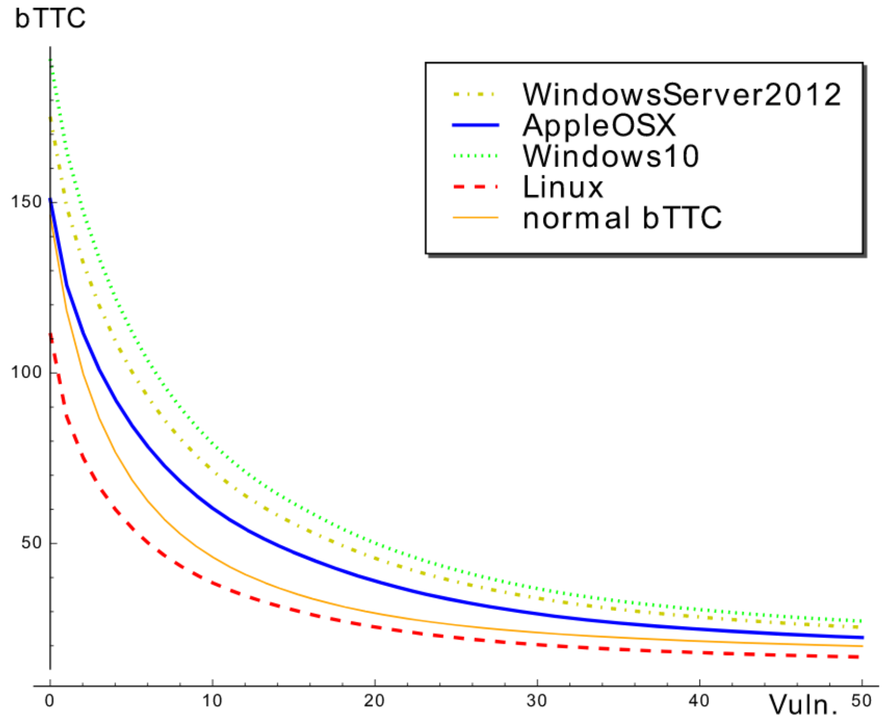


Exploit Complexity

Evaluation

Exploit complexity differs per product

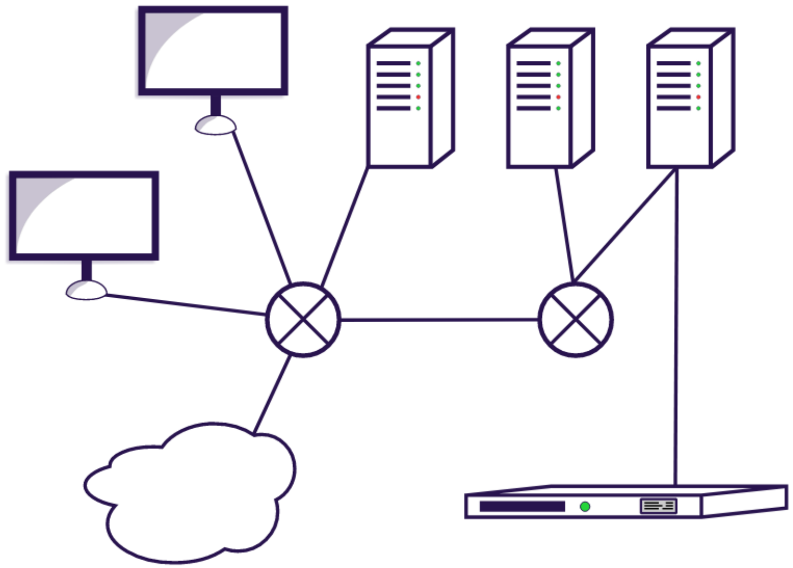




Further Work

Further CTI

Networks & complex systems



Asset Values

Thanks / Credit

Co-Authors

Felix Freiling - FAU Erlangen-Nürnberg
Klaus-Peter Kossakowski - HAW Hamburg

Resources

Clock - designed by freepik.com
Smart Mass statistics - Gartner

Critics & Corrections

Lutz Euler
Jan Kohlrausch
Sagar Gurditta
Moritz Duge
Alex Mantel