



Catching Inside Attackers

Balancing Forensic Detectability and Privacy of Employees

Jens Lindemann, Ephraim Zimmer, Dominik Herrmann,
Hannes Federrath

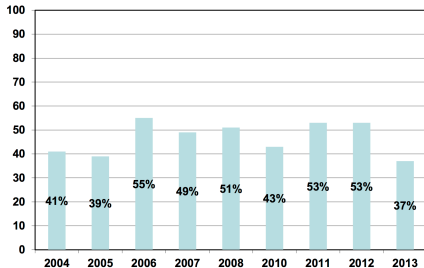
October 29, 2015



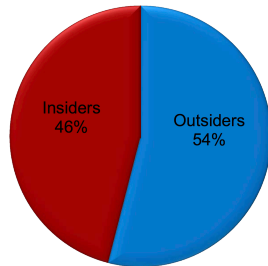
Universität Hamburg

DER FORSCHUNG | DER LEHRE | DER BILDUNG

2014 US state of of cybercrime survey [CER14]



Participants who experienced an insider incident



Electronic crimes, that were more costly or damaging

5 DEC 2012 **NEWS**

Swiss intelligence agency loses terabytes of data to an insider



Back in September the Swiss attorney general Michael Lauber and chief prosecutor Carlo Bulletti invited speculation by announcing that an employee of the Swiss intelligence services was involved in 'a serious matter of economic sabotage' posing a security threat to Switzerland, and wanted to sell stolen data 'to foreign countries.' No other countries were mentioned, and the effect was downplayed. "All the stolen data was retrieved and its transfer to third parties was prevented," reported Switzerland's news site, The Local.

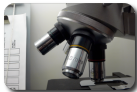


Now it emerges that the theft was larger and the potential consequences greater than originally thought. According to Reuters, "Secret information on counter-terrorism shared by foreign governments may have been compromised by a massive data theft by a senior IT technician for the NDB, Switzerland's intelligence service." Those foreign governments apparently include the US CIA and the UK's MI6, the Secret Intelligence Services that deals with foreign intelligence – both of whom routinely share intelligence with Switzerland's NDB.

It seems that the unnamed employee was an IT technician with admin rights to the entire NDB database, and was disgruntled that his input on the operation of IT services was not taken sufficiently seriously. The implication is that he acted more out of pique than in a planned act of espionage – he simply downloaded the data and walked out with it. "Investigators believe the technician downloaded terabytes, running into hundreds of thousands or even millions of printed pages, of classified material from the Swiss intelligence service's servers onto portable hard drives. He then carried them out of government buildings in a backpack," reports Reuters.

He was caught, not because of the theft, nor even because the agency's security software detected anything anomalous, but because the UBS Swiss bank became suspicious of attempts to open a new numbered bank account that was traced back to the

Agenda



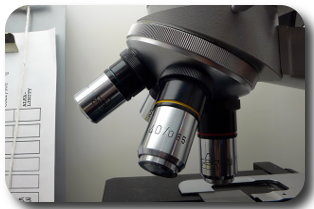
State of the art



Future research



Challenges



State of the art

Non-technical countermeasures



- Common sense guide [Sil+12]
- Main focus on motivations, opportunities and employee training
- Derived from control domains specified in Annex A of ISO 27001



Technical countermeasures

- Network-based approaches
 - Honeypots and honeytokens [Spi03]
 - Network traffic collection and analysis (ELICIT) [MS07]
- Host-based user profiling
 - Unix commandline activities [Sch+01]
 - MS Windows process table and window titles [Gol03]

Integrated approaches



- Classical security audit data & psychological data [GF10]
- Insider threat indicator ontology & processable operational context data from Human Resources [Cos+15]

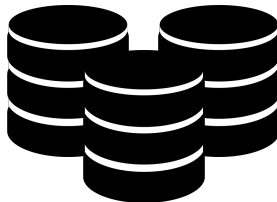


Future research

Missing bits and bytes



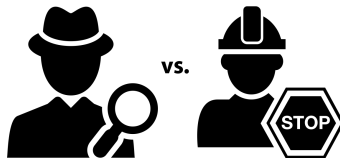
Consistent definitions



Universal datasets



Evaluation and comparison

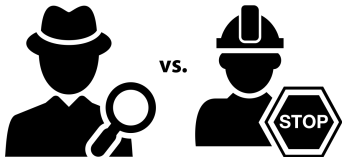


Detection vs. prevention

Prevention possible?



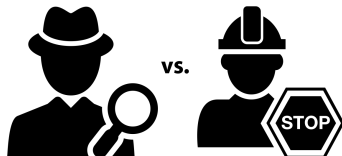
- Post-mortem detection
- Attribution
- Efficient techniques (i. e. anomaly detection)
- Reliable data sources



Prevention possible?



- Post-mortem detection
- Attribution
- Efficient techniques (i. e. anomaly detection)
- Reliable data sources

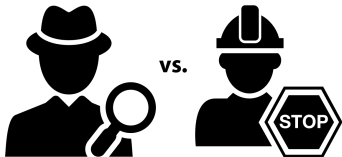


Existing work	False-positives	Detection
Honeypots [Spi03]	-	-
ELICIT [MS07]	.015	.840
Unix [Sch+01]	.014	.394
	.067	.693
Windows [Gol03]	-	-
Psychology [GF10]	-	-
Ontology [Cos+15]	-	-

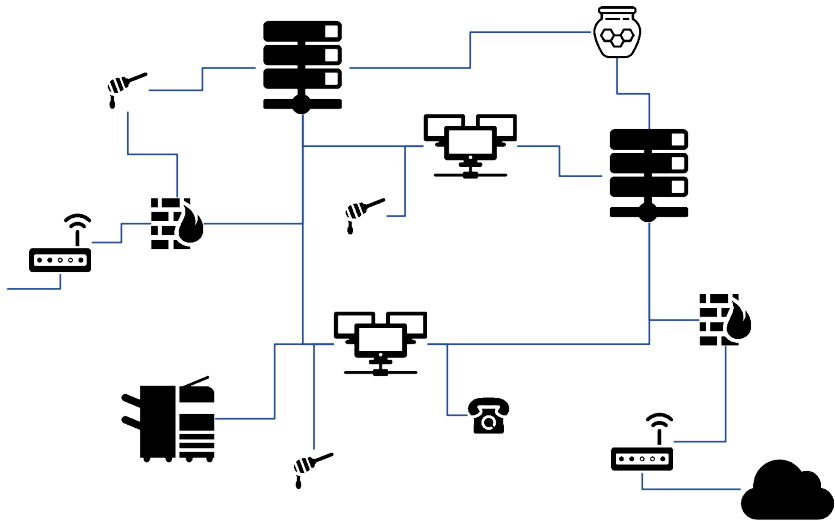
Prevention possible?



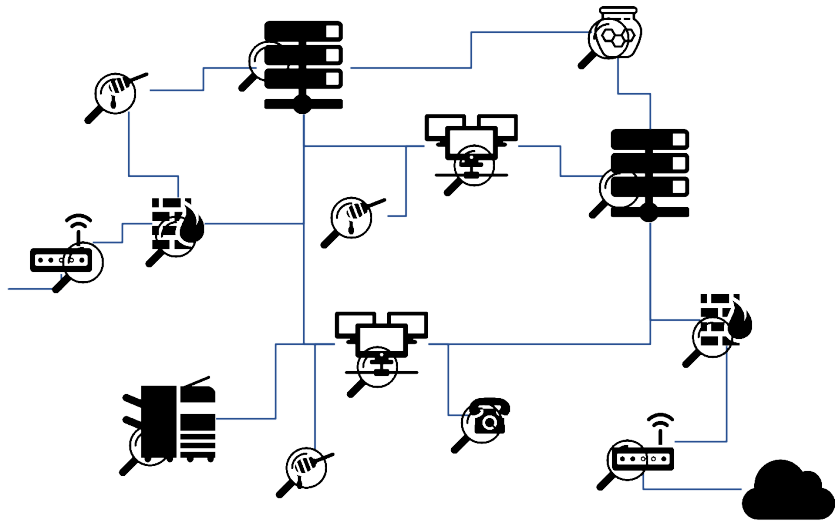
- Post-mortem detection
- Attribution
- Efficient techniques (i. e. anomaly detection)
- **Reliable data sources**



Veracity



Veracity [Go12]





Challenges

Data protection



Privacy



Detectability

- Data protection laws
- Misuse for surveillance
- Long time periods
- Linkability of behaviour to individuals
- Obfuscation

- De-anonymisation for anomaly detection
- Attribution
- Inside attacker identification



Revocable anonymity under certain conditions

Evaluation of detection / prevention techniques



- Data capture in production environments?
- Impact of anonymisation/filtering on countermeasures?
- Resembling the real world?

➡ Synthetically generated datasets

Prospects

2014 US State of Cybercrime Survey

“Only 49% of all respondents have a plan for responding to insider threats.” [MSP14]

WiK/ASW Sicherheits-Enquête 2014/2015

43% of the surveyed 160 security experts don't have strategies to counter or exacerbate data leakage. [WiK15]

Lao Tzu

"If you do not change direction, you may end up where you are heading."

Comprehensive **definitions** and consistent **terms**

Universal **datasets** of inside attacker activities
→ Comparable *evaluation*

Insider attack detection via the **veracity** concept

Tradeoff between **privacy** and **detectability**
→ *Revocable Anonymity* under certain conditions

ezimmer@informatik.uni-hamburg.de

References I



CERT Insider Threat Center. *2014 U.S. State of Cybercrime Survey*. 2014. url: <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=298318> (visited on 10/09/2015) (cit. on p. 2).



Cliparts created by Freepik and derived from Flaticon. Licensed under Creative Commons BY 3.0. url: www.flaticon.com (visited on 10/28/2015).



Daniel L. Costa et al. "An Ontology for Insider Threat Indicators". In: *10th International Conference on Semantic Technology for Intelligence, Defense, and Security (STIDS)* (2015). url: <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=426803> (visited on 09/25/2015) (cit. on pp. 8, 12).



Frank L Greitzer and Deborah A Frincke. "Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation". In: *Insider Threats in Cyber Security*. Springer, 2010, pp. 85–113 (cit. on pp. 8, 12).



Tom Goldring. "User profiling for intrusion detection in windows nt". In: *Proceedings of the 35th Symposium on the Interface*. 2003 (cit. on pp. 7, 12).



Dieter Gollmann. "Veracity, Plausibility, and Reputation". In: *Information Security Theory and Practice. Security, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems - 6th IFIP WG 11.2 International Workshop, WISTP 2012, Egham, UK, June 20-22, 2012. Proceedings*. Ed. by Ioannis G. Askoxylakis, Henrich Christopher Pöhls, and Joachim Posegga. Vol. 7322. Lecture Notes in Computer Science. Springer, 2012, pp. 20–28. isbn: 978-3-642-30954-0. doi: 10.1007/978-3-642-30955-7_3 (cit. on p. 15).

References II



Infosecurity Magazine. *Swiss intelligence agency loses terabytes of data to an insider*. 2012. url: <http://www.infosecurity-magazine.com/news/swiss-intelligence-agency-loses-terabytes-of-data/> (visited on 10/28/2015) (cit. on p. 3).



Marcus A. Maloof and Gregory D. Stephens. "ELICIT: A System for Detecting Insiders Who Violate Need-to-Know". In: *Recent Advances in Intrusion Detection*. Ed. by Christopher Kruegel, Richard Lippmann, and Andrew Clark. Vol. 4637. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2007, pp. 146–166. url: http://dx.doi.org/10.1007/978-3-540-74320-0_8 (visited on 09/21/2015) (cit. on pp. 7, 12).



Kevin Michelberg, Laurie Schive, and Neal Pollard. *US cybercrime: Rising risks, reduced readiness — Key findings from the 2014 US State of Cybercrime Survey*. 2014. url: <https://www.pwc.com/us/en/increasing-it-effectiveness/publications/2014-us-state-of-cybercrime.html> (visited on 09/24/2015) (cit. on p. 19).



Matthias Schonlau et al. "Computer Intrusion: Detecting Masquerades". In: *Statistical Science* 16.1 (2001), pp. 58–74. url: <http://www.jstor.org/stable/2676780> (visited on 09/17/2015) (cit. on pp. 7, 12).



George Silowash et al. *Common Sense Guide to Mitigating Insider Threats*. Tech. rep. CMU/SEI-2012-TR-012. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2012. url: <http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=34017> (visited on 09/24/2015) (cit. on p. 6).



Lance Spitzner. "Honeypots: catching the insider threat". In: *Computer Security Applications Conference, 2003. Proceedings. 19th Annual*. IEEE Computer Society, Dec. 2003, pp. 170–179 (cit. on pp. 7, 12).

References III



WiK - Zeitschrift für die Sicherheit der Wirtschaft, ASW Bundesverband. *WiK/ASW Sicherheits-Enquête 2014/2015*. 2015. url: <http://www.wik.info/2015/06/1412/> (visited on 10/28/2015) (cit. on p. 19).