Your Seminar Paper Title/Titel der Seminararbeit

Your Name/Ihr Name (Matrikelnummer auf einem separaten Blatt abgeben)
htw saar – Hochschule für Technik und Wirtschaft des Saarlandes
Seminar "Angewandte Informatik/Computer Science and Society" (je nach Seminar anpassen)
{Winter,Sommer}semester 20xx

***Abstract*—Your abstract goes here. Please consider Kent Beck's recommendations for writing an abstract.**

I. Introduction / Einführung

Beispiele für Zitate: [1], [2], [3], [4], [5], [6]

A. Szenario

A concrete, but simple example from the *financial services domain* is a generic trading process, e.g., in investment banking, where market data such as interest rates and ratings are retrieved from external agencies for deal pricing calculations (cf. Figure 1). Just by monitoring the message exchange between the bank and the agencies, an attacker can gain information about the amount of requests for the internal deal calculations, when the bank works on its deals, and so on.

If more complex service compositions can be observed, e.g., if successful deals are processed by transaction services, attackers can also infer information about transactions closed successfully in general – among which are also successfully closed deals. This is easily available, but very sensitive information that is not protected by the currently used Web service security technology. However, standard anonymity mechanisms are available for communication systems which could be used until dedicated solutions are available, i.e., taking into account the high Quality of Service (QoS) requirements of Web service communication.

A concrete, but simple example from the financial services domain is a generic trading process, e.g., in investment banking, where market data such as interest rates and ratings are retrieved from external agencies for deal pricing calculations (cf. Figure 1). Just by monitoring the message exchange between the bank and the agencies, an attacker can gain information about the amount of requests for the internal deal calculations, when the bank works on its deals, and so on. If more complex service compositions can be observed, e.g., if successful deals are processed by transaction services, attackers can also infer information about transactions closed successfully in general – among which are also successfully closed deals. This is easily available, but very sensitive information that is not protected by the currently used Web service security technology. However, standard anonymity mechanisms are available for communication systems which could be used until dedicated solutions are available, i.e., taking into account the high Quality of Service (QoS) requirements of Web service communication.

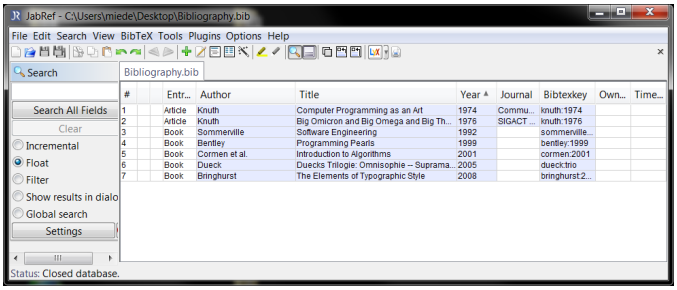

Figure 1. Screenshots should be in PNG format, general photos in JPG, and diagrams etc. as PDF (vector).

Table I
Global distribution of Web service providers used for the experiments.

Country	*Web service provider*
USA	`www.webservicex.com`
USA	`ws.cdyne.com`
USA	`www.kbb.com`
Australia	`national.atdw.com.au`
Great Britain	`dw.sheetmusicdirect.com`
The Netherlands	`artselect.artikelbeheer.nl`
Canada	`netpub.cstudies.ubc.ca`
Russia	`www.cbr.ru`
China	`www.sircweb.cn`
Brazil	`ws.cronostelemetria.com.br`
Germany	`mathertel.de`

In total, we choose eleven different Web services from distinct and globally distributed providers as shown in Table I.

Just by monitoring the message exchange between the bank and the agencies, an attacker can gain information about the amount of requests for the internal deal calculations, when the bank works on its deals, and so on. If more complex service compositions can be observed, e.g., if successful deals are processed by transaction services, attackers can also infer information about transactions closed successfully in general – among which are also successfully closed deals.

II. Related Work / Stand der Technik

A concrete, but simple example from the financial services domain is a generic trading process, e.g., in investment banking, where market data such as interest rates and ratings are retrieved from external agencies for deal pricing calculations (cf. Figure 1). Just by monitoring the message exchange

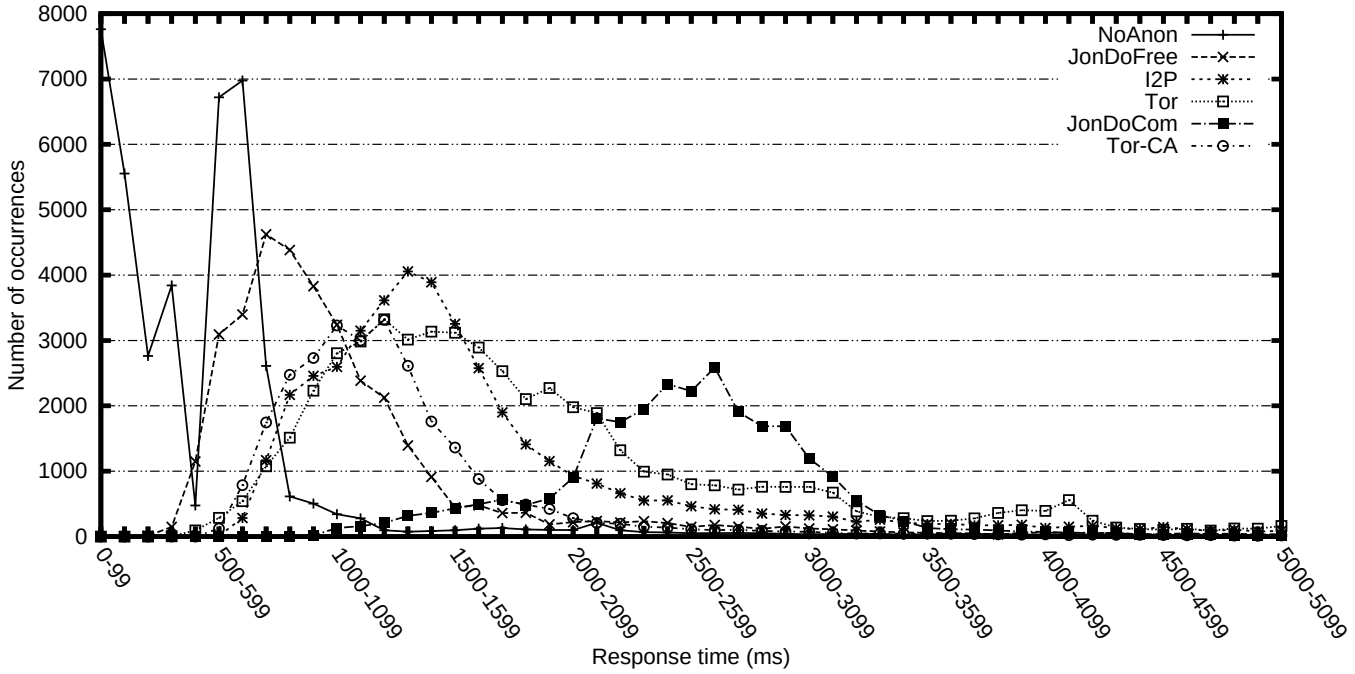

Figure 2. Overall number of measured response times per anonymity system.

between the bank and the agencies, an attacker can gain information about the amount of requests for the internal deal calculations, when the bank works on its deals, and so on. If more complex service compositions can be observed, e.g., if successful deals are processed by transaction services, attackers can also infer information about transactions closed successfully in general – among which are also successfully closed deals. This is easily available, but very sensitive information that is not protected by the currently used Web service security technology. However, standard anonymity mechanisms are available for communication systems which could be used until dedicated solutions are available, i.e., taking into account the high Quality of Service (QoS) requirements of Web service communication.

III. ...

A concrete, but simple example from the financial services domain is a generic trading process, e.g., in investment banking, where market data such as interest rates and ratings are retrieved from external agencies for deal pricing calculations (cf. Figure 1).

IV. Summary and Outlook / Zusammenfassung und Ausblick

A concrete, but simple example from the financial services domain is a generic trading process, e.g., in investment banking, where market data such as interest rates and ratings are retrieved from external agencies for deal pricing calculations (cf. Figure 1). Just by monitoring the message exchange between the bank and the agencies, an attacker can gain information about the amount of requests for the internal deal calculations, when the bank works on its deals, and so on. If more complex service compositions can be observed, e.g., if successful deals are processed by transaction services, attackers can also infer information about transactions closed successfully in general – among which are also successfully closed deals. This is easily available, but very sensitive information that is not protected by the currently used Web service security technology. However, standard anonymity mechanisms are available for communication systems which could be used until dedicated solutions are available, i.e., taking into account the high Quality of Service (QoS) requirements of Web service communication.

References

[1] B. Schneier, *Secrets and Lies: Digital Security in a Networked World*, 1st ed. Wiley, 1 2004.

[2] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. Wiley, 4 2008.

[3] C. Eckert, *IT-Sicherheit: Konzepte – Verfahren – Protokolle*, 5th ed. Oldenbourg, 11 2007.

[4] J. D. Howard and T. A. Longstaff, "A Common Language for Computer Security Incidents," Sandia National Laboratories, Sandia Report SAND98-8667, 10 1998.

[5] A. Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt*, 1st ed. Addison-Wesley Professional, 4 2007.

[6] B. Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World.* Springer, 5 2003.