HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Kurzfassung der Diplomarbeit

Abteilung	**Informatik**
Name der Diplomandin / des Diplomanden	**Roland Räz** **Reto Meier**
Diplomjahr	**2001**
Titel der Diplomarbeit	**DNS Security**
Examinatorin / Examinator	**Ivan Bütler, Compass Security AG**

Kurzfassung der Diplomarbeit

Immer wieder liest man in Zeitungen und Fachzeitschriften von Hack-Angriffen auf Naming Services. Der im Internet am weitesten verbreitete Naming Service ist der des DNS (Domain Name System). Dieser ist für die Umsetzung zwischen Domain Namen, z.B. www.hsr.ch, und der für Rechner eindeutigen IP-Adresse zuständig. Die Auswirkungen einer erfolgreichen Attacke können verheerend sein. Es kann zum Beispiel passieren, dass Webseiten über längere Zeit nicht mehr erreichbar sind, oder dass man auf eine manipulierte Seite umgeleitet wird, ohne etwas davon zu merken. Hacker können mit Hilfe von DNS-Spoofing Attacken an persönliche Daten von Internetbenützern kommen oder sogar deren E-Mail-Verkehr umleiten.

In dieser Diplomarbeit wird, im Auftrag der ***Compass Security AG***, das Thema "DNS und Sicherheit" analysiert und die Ergebnisse in einer Publikation auf dem Internet veröffentlicht. Zudem soll ein Democase implementiert werden, mit welchem eine Attacke auf einen DNS-Server durchgeführt werden kann.

In der Bedrohungsanalyse der Publikation werden unter anderem folgende Attacken beschrieben:

Cache Poisoning:
Der Hacker nutzt eine Sicherheitslücke eines DNS-Servers aus und "vergiftet" den Cache mit falschen Einträgen.

Query-ID-Prediction:
Jede Anfrage (Query) an einen DNS-Server beinhaltet eine ID, mit welcher der Client die zurückkommenden Antworten seinen Anfragen zuordnen kann. Wenn der Hacker diese ID vorhersagen kann, kann er solche Anfragen anstelle des DNS-Servers mit falschen Daten beantworten.

"Man in the middle"-Attacke:
Bei dieser Attacke positioniert sich der Hacker zwischen Client und DNS-Server und hört die Datenverbindung ab. Er kann die Daten nach Belieben ändern, ohne dass jemand etwas merkt.

Administrations-Attacke:
Nicht zu vergessen ist die Attacke, bei welcher der Hacker, aufgrund mangelhafter Authentisierung, bei der Registrierungsstelle probiert eine Änderung der Domain-Registrierung eines Opfers vorzunehmen. Z.B. mit einer gefälschten E-Mail.

Die zuständigen Institutionen sind vor allem seit den Ereignissen am 11. September 2001 in New York daran, die Sicherheit von DNS zu verbessern und der schon seit 1997 bekannte Standard DNSSec einzuführen.