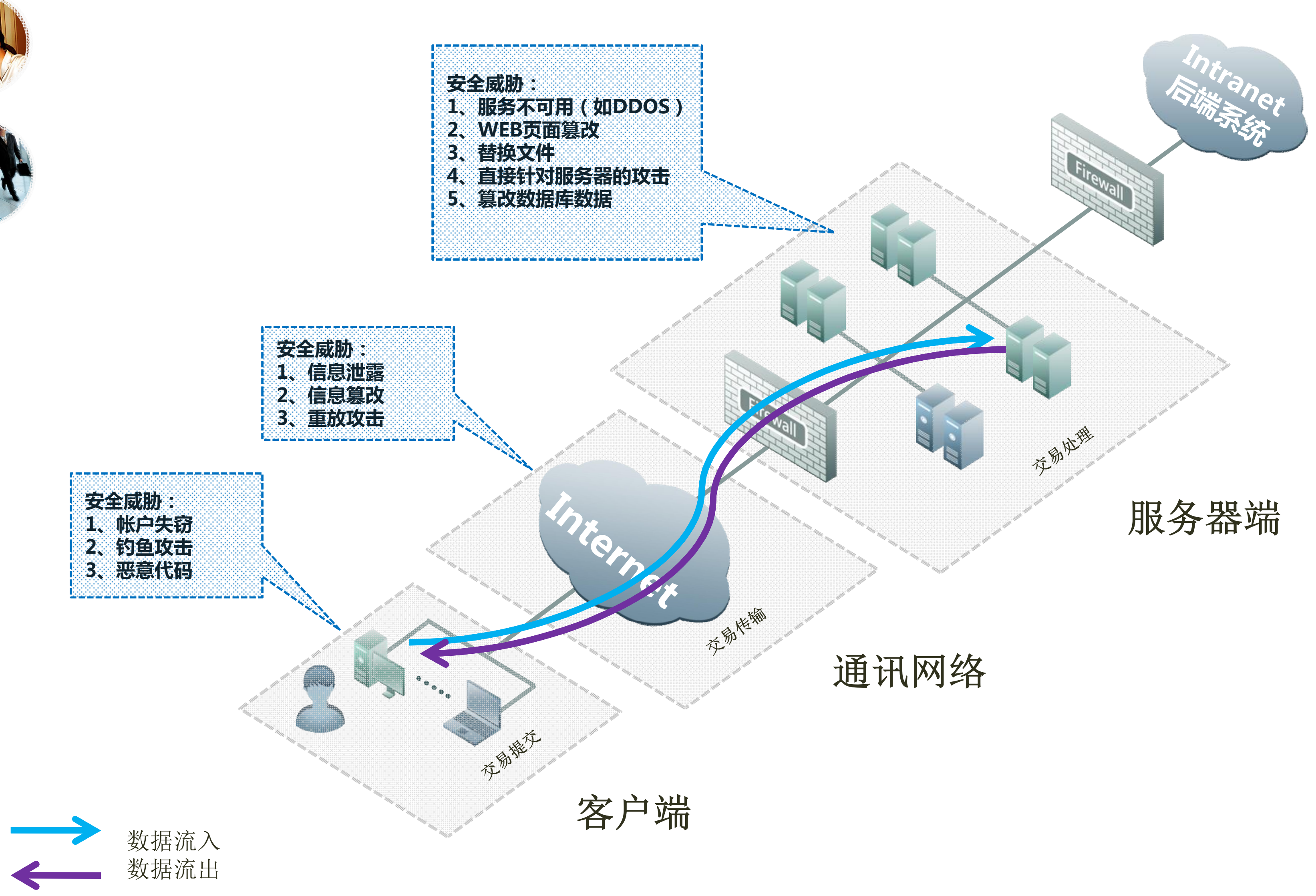
几个攻击实例

- 网上银行安全威胁
- 利用**search engine**的信息收集
- 利用云计算的**DOS**攻击（演示）
- 利用**SNS**的**BOTNET**
- 控制胰岛素泵 **(**课外阅读）
- 利用人计算的**CAPTCHA(Completely Automated Public Turing test to tell Computers and Humans Apart)**破解
- **APT Attack to RSA SecureID**
- 攻击**VOIP**
- 攻击**MPLS** 。。。
- **Wifi** 攻击**: wifi advanced fuzzing,blackhat EU2007**

http://samy.pl

攻击方法不断演进和创新

网上银行系统安全威胁



安全威胁：
1、服务不可用（如DDOS）
2、WEB页面篡改
3、替换文件
4、直接针对服务器的攻击
5、篡改数据库数据

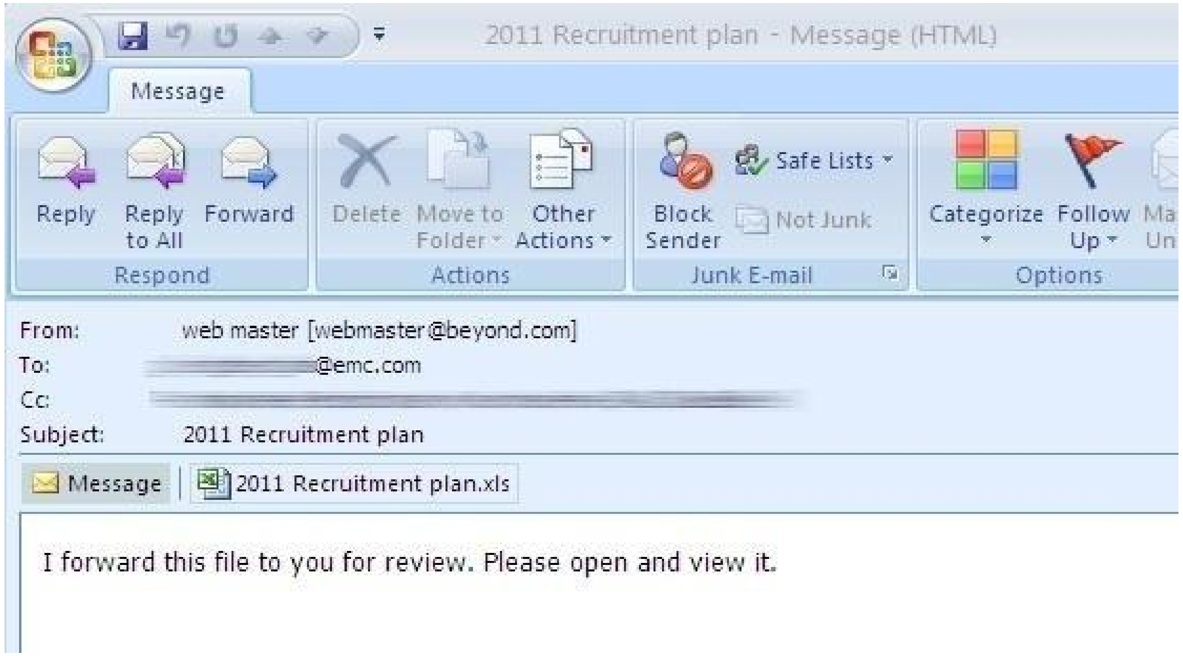
安全威胁：
1、信息泄露
2、信息篡改
3、重放攻击

安全威胁：
1、帐户失窃
2、钓鱼攻击
3、恶意代码

→ 数据流入
← 数据流出

Courtesy: NSfocus

APT Attack to RSA SecureID



2011 Recruitment plan - Message (HTML)

From: web master [webmaster@beyond.com]

To: [redacted]@emc.com

Cc: [redacted]

Subject: 2011 Recruitment plan

Message | 2011 Recruitment plan.xls

I forward this file to you for review. Please open and view it.

Our investigation has revealed that the attack resulted in certain informatior being extracted from RSA’s systems. Some of that information is related to RSA’s SecurID two-factor authentication products. While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack.

1） 攻击者给RSA的母公司EMC的4名员工发送了两组恶意邮件。邮件标题为“2011 Recruitment Plan”，寄件人是webmaster@Beyond.com，正文很简单，写着“I forward this file to you for review. Please open and view it.”；里面有个EXCEL附件名为“2011 Recruitment plan.xls”；

2） 很不幸，其中一位员工对此邮件感到兴趣，并将其从垃圾邮件中取出来阅读，殊不知此电子表格其实含有当时最新的Adobe Flash的0day漏洞（CVE-2011-0609）。这个Excel打开后啥也没有，除了在一个表单的第一个格子里面有个“X”（叉）。而这个叉实际上就是内嵌的一个Flash。

3） 该主机被植入臭名昭著的Poison Ivy远端控制工具，并开始自BotNet的C&C服务器（位于 good.mincesur.com）下载指令进行任务；（内网IDS？？？）

4） 首批受害的使用者并非“位高权重”人物，紧接着相关联的人士包括IT与非IT等服务器管理员相继被黑；

5） RSA发现开发用服务器（Staging server）遭入侵，攻击方随即进行撤离，加密并压缩所有资料（都是rar格式），并以FTP传送至远端主机，又迅速再次搬离该主机，清除任何踪迹；

6）在拿到了SecurID的信息后，攻击者就开始对使用SecurID的公司（例如上述防务公司等）进行攻击了。

安全建模

- 攻击树
- 攻击图
- 博弈论
- Petri 网

关于攻击和威胁模型：

- 攻击树模型
  - a systematic method to characterize system security based on varying attacks. Each attack tree enumerates and elaborates the ways that an attacker could cause the event to occur. Each path through an attack tree represents a unique attack
  - 攻击树attack tree用来建模攻击有可能发生的过程
  - 根节点是攻击目标，然后将根节点分解为一系列子目标，再将子目标分解直到叶子节点。叶子节点代表单独的攻击者行为。这种攻击树结构的子结点之间有AND,OR和CAND的关系。
- Edge, K.S.; Dalton, G.C.; Raines, R.A.; Mills, R.F. Using Attack and Protection Trees to Analyze Threats and Defenses to Homeland Security. Military Communications Conference, 2006. MILCOM 2006
- Gan, Zaobin; Tang, Jiufei; Wu, Ping; Varadharajan, Vijay.A Novel Security Risk Evaluation for Information Systems. Frontier of Computer Science and Technology, 2007. FCST 2007. Japan-China Joint Workshop on1-3 Nov. 2007 Page(s):67 – 73

This introductory article is good: John Viega and Gary McGraw, Attack Trees Software Development, August 2002. It includes a partial attack tree for SSH.

Bruce Schneier, Attack Trees Dr. Dobb's Journal, December 1999. Also this figure: Attack Nodes. This may also be the Dr. Dobb's reference.

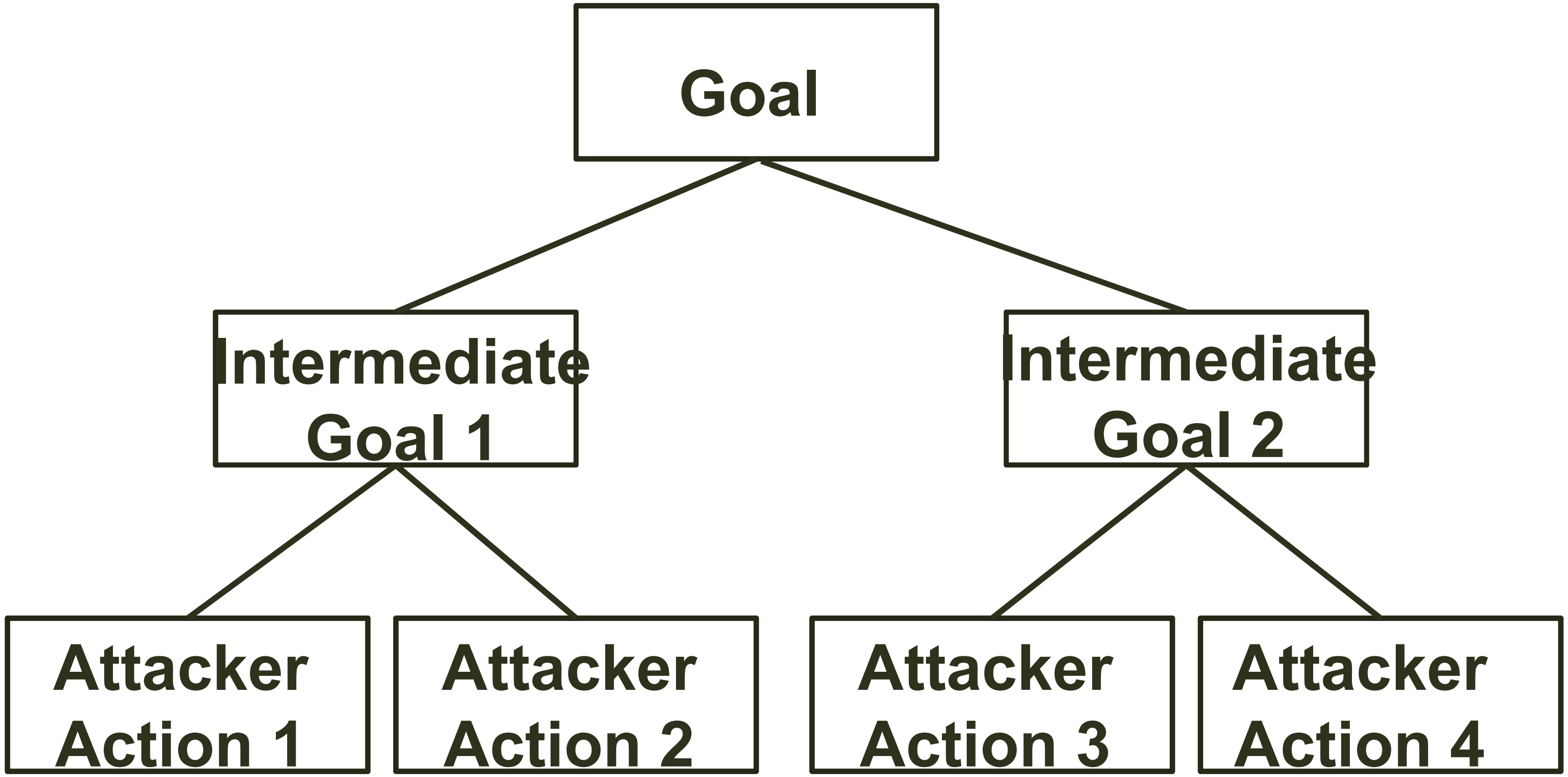
Bruce Schneier, Secrets and Lies chapter 21.

Moore, Ellison and Linger of CMU/SEI have written quite a serious 'manual' MEL of how to do attack modeling using attack trees. It is certainly worth reading.

A mister Moberg has written his thesis on an attack tree model for Lotus Notes I hadn't had the time for a careful read, but skimming its contents suggest that it is quite informative. It is the only serious analysis I've found of a live/existing product of any size.

In Niels Ferguson's book the "safe-cracking" example in chapter 1 probably hasn't escaped your attention. Although I do agree that it is a trivial example.

draft-convery-bgpattack-00 (Convery, Cook, Franz) (IETF draft presenting all known attack vectors into or using BGP, presented in "Attack Tree" format.)



Goal

Intermediate Goal 1

Intermediate Goal 2

Attacker Action 1

Attacker Action 2

Attacker Action 3

Attacker Action 4

- 为了达到攻击目的可以完成(Action 1 OR Action 2) OR(Action 3 AND Action 4)

为了恰当的分析攻击树模型，需要让每个节点有一定的度量，比如攻击成功的概率，攻击代价，系统影响和风险等。度量首先被赋到叶子节点，因为只有叶子节点才是攻击者实际可控的。上层节点的度量是根据下层节点**AND** 或**OR**的关系计算出来的。

如：

	AND	OR
Probalality	$\prod_{i=1}^{n} prob_i$	1-$\prod_{i=1}^{n}(1 - prob_i)$
Cost	$\sum_{i=1}^{n} cost_i$	$\frac{\sum_{i=1}^{n} prob_i * cost_i}{\sum_{i=1}^{n} prob_i}$
Impact	$\frac{10^n - \prod_{i=1}^{n}(10 - impact_i)}{10^{(n-1)}}$	$\max_{1 \le i \le n} impact_i$

保护树protect tree

- 通过指定一个特定的保护作为节点或者子树，保护树可以产生一个应该在哪里进行保护的分析，以用最少的资源支出获得最大的保护。保护树的根节点直接对应攻击树的根节点，但是剩下的部分可能会有很大的不同。
- 另外，可以提前修剪攻击树，这是在对攻击者能力假设的基础上进行的，超过设想的能力范围就认为不会被攻击。

练习： 画出一个攻击树，如：针对个人主机

Tools

Amenza SecuriTree - *SecurITree's capabilities-based attack tree analysis works in a broad variety of disciplines ranging from information technology to physical security. Amenaza's customers include defense and intelligence organizations, health care providers, critical infrastructure companies, aerospace manufacturers, financial organizations, laboratories, consulting companies and progressive Fortune 1000 clients. Throw away your obsolete hostile risk analysis methodologies and model the future of your security.*

Microsoft Threat Modeling Tool - *The Threat Modeling Tool allows users to create threat model documents for applications. It organizes relevant data points, such as entry points, assets, trust levels, data flow diagrams, threats, threat trees, and vulnerabilities into an easy-to-use tree-based view. The tool saves the document as XML, and will export to HTML and MHT using the included XSLTs, or a custom transform supplied by the user.*

Microsoft Threat Analysis & Modeling v2.0 BETA2 - *Microsoft Threat Analysis & Modeling tool allows non-security subject matter experts to enter already known information including business requirements and application architecture which is then used to produce a feature-rich threat model.*

Attack graph

- Swiler和Phillips 在1998年提出来，基于model checker的网络脆弱性分析技术
- 基于图论理论的攻击模型，描述从攻击发起者到攻击目标所有路径的一种有向图。
- can reveal potential threats by enumerating all possible sequences of exploits that an attacker can follow to compromise given critical resources.
- An Attack Path specifies an attack scenario that results in compromising organization values. It tells us how an attacker gains access to the victim computer; how and which vulnerability attacker can take advantage of and what kind of damage may be done that can impact the organization.

- 攻击图主要分为状态攻击图和属性攻击图两类。
- 状态攻击图中的节点表示网络的当前状态，网络状态信息包括主机相关信息、用户权限、主机提供的服务等信息。有向边表示引起状态改变的攻击行为。
- 属性攻击图有两类节点，一类代表原子攻击，另一类是属性节点，代表原子攻击的前提或结果。连接属性节点与原子攻击节点之间的边称为前提边或者后果边。只有当所有通过前提边与原子攻击节点相连的属性都被满足时，该原子节点所代表的原子攻击才会被执行。

- 例：
  - 如何利用安全模型进行威胁分析
    - S_Threat analysis – a case study smart metering.pdf
    - Using Threat modeling to design secure applications.PDF