مبانی رایانش امن
بویش-جعل-جاسوسی-حملات بندآوری خدمت

محسن هوشمند
دانشکده تکنولوژی اطلاعات و علم رایانه
دانشگاه تحصیلات تکمیلی علوم پایه زنجان

بویایی SNIFFING و جاسوسی SNOOPING- جعل SPOOFING

آغاز اکثر حملات با ادراک ترافیک شبکه

- فرض بر حضور مهاجم در شبکهٔ قربانی
- مثال- استفاده از لبتاپ در رنج شبکه بی‌سیم قربانی
- یا دسترسی به پی‌سی در شبکه سیمی

سادگی بویایی روی رسانهٔ همگانی

- مانند بی‌سیم WiFi یا پیاده‌سازی اترنت
- صرفا شنود جریان بیت‌های عبوری
- در حالت دریافت هر بسته قرار دادن promiscuous mode نه نمی‌گوید! پذیرش تمامی بسته‌ها در کانال
- استفاده از tcpdump یا Wireshark جهت دریافت ترافیک

بویایی در شبکه‌های سوییچی

عدم سادگی بویایی در بسیاری از شبکه‌ها

اترنت جدید

- تفاوت با جدش
- نبودن تکنولوژی شبکه رسانه-اشتراکی
- سوییچ شدن تمامی ارتباطات
- عدم دریافت هیچ قاب اترنت با مقصد میزبان‌های دیگر توسط مهاجم
- خودآموز بودن سوییچ‌های اترنت و تشکیل سریع جدول پیش‌فرستی؟ forwarding
- با دریافت ترافیک میزبان الف روی درگاه ۱ سوییچ، تخصیص درگاه منظور به میزبان مذکور
  - تخصیص دیگر پورت‌ها به طریق مشابه
  - عدم ارسال داده پورتی خاص به دیگر پرت‌ها به محض کامل شدن جدول پیش‌فرستی

بویایی در شبکه‌های سوییچی

- وجود روش‌های متفاوت برای غلبهٔ مهاجم بر مشکل سوییچ‌کردن
  - استفادهٔ تمامی از جاسوسی
- MAC cloning کپی کردن نشانی MAC میزبانی که قصد بویایی آن هست
- ادعای دارا بودن نشانی MAC
  - چگونه؟ با ارسال قاب‌های اترنت با همان نشانی
  - ضبط رکورد منظور در سوییچ و ارسال تمامی ترافیک قربانی به روی ماشین شما.
    - با فرض دانستن نشانی
    - امکان دریافت آن با درخواست‌های ARP که هدف برای تمامی میزبان‌ها در قطعه شبکه ارسال می‌کند.
    - عامل پیچیدهٔ دیگر: حذف برچسب شما از سوییچ به محض ارتباط دوباره صاحب اصلی نشانی مک
    - نیاز به تکرار مداوم مسموم‌سازی جدول سوییچ switch table poisoning
- روش دیگر
  - اندازهٔ محدود جدول سوییچ و خفه کردن سوییچ با قاب‌های فریم با نشانی مبدا جعلی
  - عدم درک سوییچ از جعلی بودن نشانی‌های مک و ضبط آنها تا پر شدن جدول
  - حذف مدخل‌های قدیمی‌تر جهت جانشانی مک‌های جدید
  - به دلیل عدم وجود مدخل برای میزبان هدف، همه‌پخشی ترافیک
    - سیل مک MAC flooding
    - تبدیل اترنت به رسانهٔ اشتراکی پنجاه و چند سالهٔ پیش

بویایی در شبکه‌های سوییچی

- راه دیگر به جای گیج کردن سوییچ
- هدف قرار دادن میزبان‌ها مستقیما با حملهٔ جاسوسی ارپ یا مسموم‌سازی ارپ **ARP spoofing** یا **ARP poisoning**
- یادآوری: ارپ پروتکل یاور رایانه جهت یافتن نشانی MAC متناظر با نشانی IP
- ارپ فراهم‌ساز جدول نگاشت آی‌پی به مک تمامی میزبان‌های در ارتباط با ماشین
  - جدول ارپ
- هر مدخل دارای زمان زندگی حدود دقایق
- حذف مواردی که زمان زندگی به صفر برسد
- تمامی ارتباطات در درجهٔ نخست نیازمند جستجوی ارپ
  - بدنبال نشانی مک میزبانی با آی‌پی مشخص
  - مهاجم به محض دیدن درخواست ارپ برای میزبان دیگر، پاسخ به درخواست دهنده
  - به دلیل سادگی و بی حافظگی پیاده‌سازی ارپ
    - امکان ارسال پاسخ ارپ در زمان نبود هیچ درخواست.
    - جدول ارپ آن را می‌پذیرد.
- مهاجم دریافت کنندهٔ ترافیک بین دو طرف در ارتباط با عامل ترفند مذکور برای هر دو
- سپس ارسال قاب‌ها برای نشانی‌های صحیح مک
  - پیاده‌سازی نشسته در میان MITM
  - امکان دریافت ترافیک بین دو میزبان

جعل (فارغ از ارپ)

جعل spoofing ارسال بایت‌ها در شبکه با نشانی مبدأ غلط

نیاز به جعل بسته‌ها و دیگر ترافیک‌ها علاوه بر بسته‌های ارپ

مثال SMTP

- پروتکل متن‌محور مورداستفاده در همه جا جهت ارسال ایمیل
- امکان تغییر فرستنده در آن
- ارسال تمامی پاسخ‌ها به نشانی مذکور
- استفاده از ایمیل جهت ایمیل‌های طله

جعل ارپ در لایه پیوند داده

جعل SMTP در لایهٔ کاربرد

- به طریق اولی امکان جعل در هر لایه‌ای
- امکان ایجاد قاب اترنت، دیتاگرم آی‌پی یا بسته UDP
- کفایت تغییر نامه نشانی مبدأ
- عدم وجود راهی برای تشخیص دغل

جعل (فارغ از ارپ)

چالشی‌تر بودن دیگر پروتکل‌ها

- مثلا TCP
  - میزبان‌ها اتصال تی‌سی‌پی حفظ حالت مانند شماره دنباله و تایید
  - سخت‌تر شدن جعل
  - راه‌حل: بوییدن یا حدس شماره دنبالهٔ صحیح
- امکان استفاده از پروتکل‌های ساده‌تر برای آسیب مثلا استفاده از بسته‌های UDP برای حملات بندآوری خدمت

جعل DNS

استفاده از UDP جهت درخواست‌ها و پاسخ‌ها

همانند جعل ارپ: انتظار برای ارسال درخواست جستجو از طرف مشتری

- رقابت با سیستم نام دامنه جهت تحویل پاسخ غلط
- سعی بر نمایش آی‌پی موردنظر شما
  - بوییدن ترافیک کاربر
  - مشکلات
    - عدم امکان دیدن پیام در تمامی مواقع
    - عدم مفید بودن جعلی دی‌ان‌اس هنگام رویت تمامی ترافیک

جعل DNS

راه دیگر

- در صورت داشتن سرور نام محلی کاربر
- ارسال تقاضا به سرور نام
- سرور محلی جستجو از سطح بالاتر سرور نام
- پاسخ جعلی سریع مهاجم به درخواست بین سرورها
- ذخیره نگاشت غلط در سرورهای محلی و تحویل آن به کاربران
- ایراد شناسه ۱۶ بیتی درخواست و پذیرش پاسخ در صورت تطبیق شناسه
- مهاجم در صورت ندیدن درخواست
  - نیاز به حدس شناسه از بین ۶۵۵۳۶ مورد
  - نیاز به ارسال هزاران پاسخ DNS در زمان کم و بدون برانگیختن توجه

جعل DNS

راه ساده‌تر

- حمله تولد
- نیاز به چند نفر در کلاس داریم تا احتمال تولد دو نفر در یک روز بیشتر از پنجاه در صد باشد؟
  - ؟
  - ۲۳
- تعمیم: وجود نگاشت بین ورودی و خروجی با n ورودی و k خروجی
- به جای بررسی تطبیق تولد یک نفر بررسی، مقایسهٔ همه با همه و هر تطبیق ممکن بین آنها

مهاجم ارسال صدها درخواست DNS درابتدای امر برای درخواست دامنه‌ای که قصد تغییرش را دارند.

سرور نام محلی به دنبال حل درخواست‌ها با پرسش از سرور رده بالاتر

ارسال فی‌الفور صدها پاسخ جعلی برای هر درخواست، پس از ارسال درخواست‌ها

- تظاهر به پاسخ از سرور رده بالاتر و هر کدام دارای شناسه متفاوت
- با مسموم کردن سرور نام محلی برای وب سایت خاص
  - دسترسی مهاجمان به ترافیک ارسالی به آن از طرف تمامی کاربران سرور نام
  - رله‌سازی دوبارهٔ تمامی ارتباطات از طرف مشتری به سرور: نشسته در میان

حملهٔ کامینسکی

بدتر شدن مراتب با مسموم‌سازی تمامی ناحیه به جای تک تارمانه

- معروف به حمله DNS دن کامینسکی
- درخواست جستجو DNS نشانی آی‌پی **www,cs,vu.nl**
- با دریافت درخواست ارسال درخواست به سرور ریشه یا سرور سطح بالای نام دامنهٔ **.nl**
  - غالبا مورد اخیر

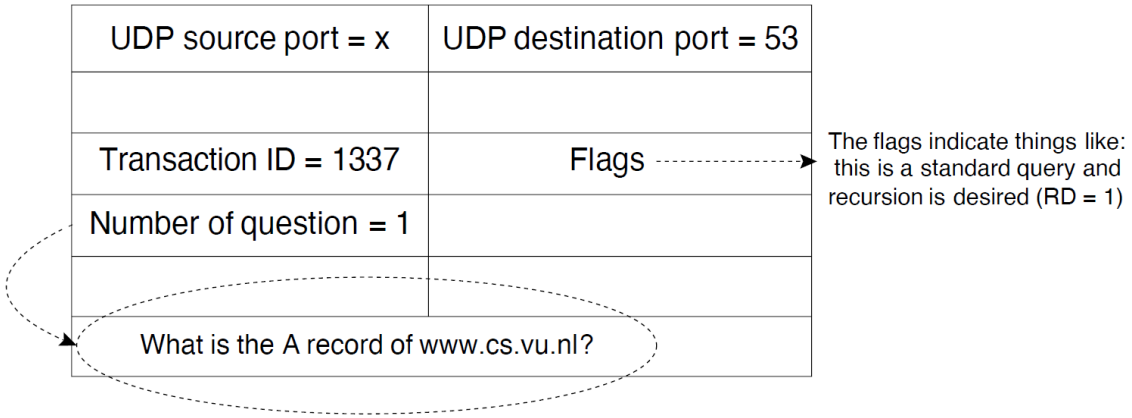

Figure 8-3. A DNS request for *www.cs.vu.nl*.

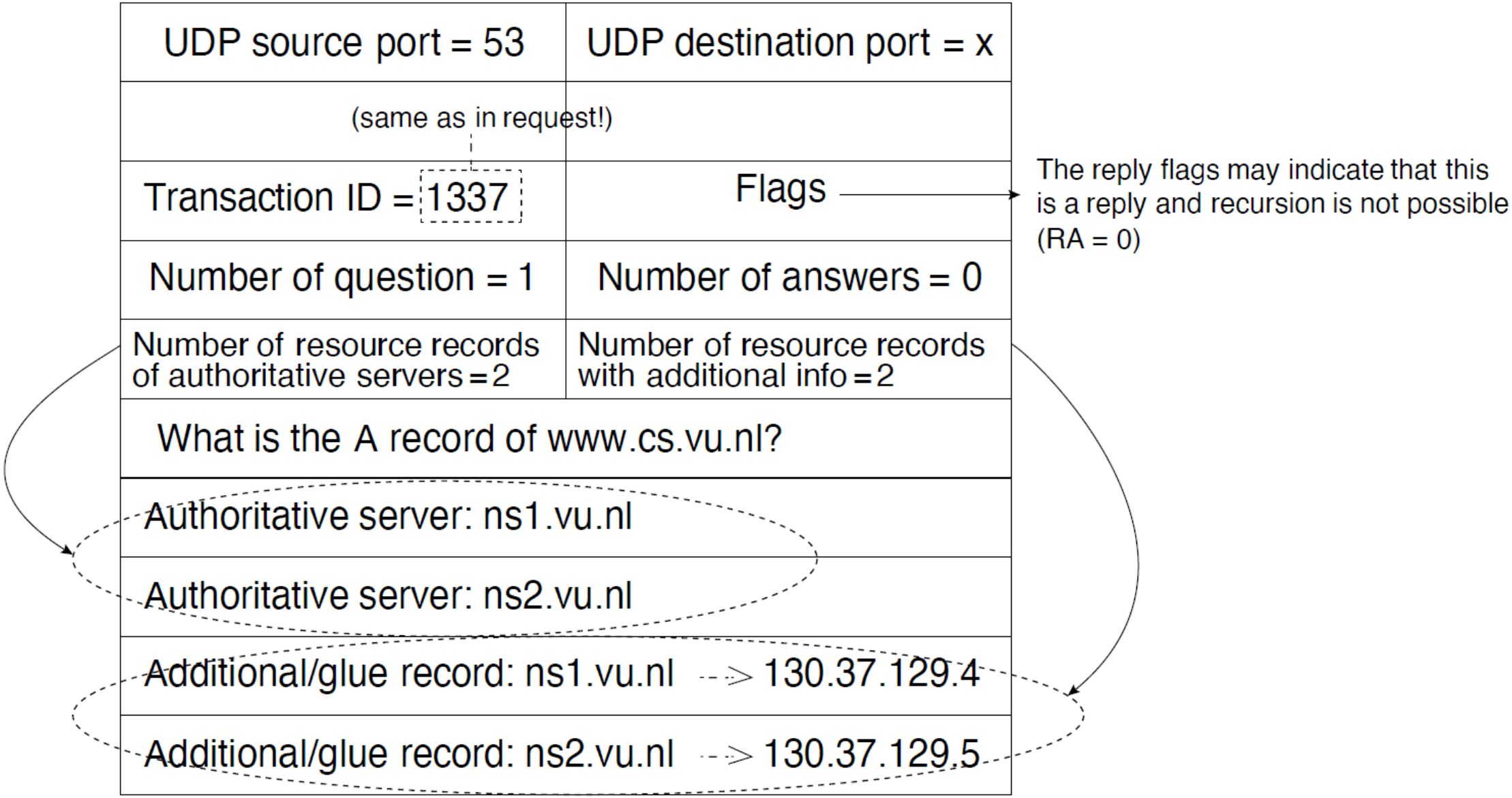

Figure 8-4. A DNS reply sent by the TLD name server.

حملهٔ کامینسکی

عمل مهاجمان

- ارسال درخواست جستجو برای زیردامنه غیرموجود در دامنه دانشگاه
- عدم وجود زیردامنه، هیچ سرور نامی قادر به نگاشت نیست
- سرور نام محلی تماس با سرور نام TLD
- ارسال پاسخ‌های جعلی فراوان پس از ارسال درخواست‌ها همانند جعل DNS
  - با این تفاوت که سرور TLDپاسخ را نمی‌داند.
  - عدم انجام جستجوی بازگشتی و پاسخ به سرور محلی برای تماس با سرور نام دانشگاه جهت تکمیل درخواست جستجو
  - امکان پاسخ سرورنام‌ها به سرور محلی
  - تنها مورد مغلوط‌سازی رکوردهای گلو به نشانی آی‌پی که آنها کنترل می‌کنند.
  - مهاجم به مثابهٔ نشسته در میانی برای هر سایت در دامنهٔ دانشگاه
- آسیب‌پذیری بسیاری از سرورهای نام به نوع حمله
- راه‌حل؟
  - یادآوری ۱۶ بیتی بودن شناسه: افزودن طول شناسه؟ خیر! سختی تغییر پیام پروتکل DNS
    - معرفی تصادفی بودن در درگاه مبدا UDP
    - مهاجم نیاز به حدس شناسه و درگاه مبدا UDP
  - DNSSEC
    - مجموعه‌ای از گسترش‌های DNS

جعل TCP

پیچده‌تر بودن جعل TCP

در صورت تظاهر به آمدن قطعه تی‌سی‌پی از کامپیوتر دیگر نیاز به حدس شماره درگاه و شماره دنبالهٔ صحیح

جعل اتصال: برقرار کردن اتصال جدید و تظاهر به شخصی غیر بودن در کامپیوتر دیگر

- حملهٔ کوین میتنیک به مرکز ابرمحاسبات سن دیگو در روز کریسمس ۱۹۹۴

ربایش اتصال: ورود داده در اتصال بین دو طرف و تظاهر به هر دو طرف مذکور

جعل تی‌سی‌پی –مرکز محاسبات سن دیگو

حمله در روز کریسمس؟

با شناسایی اولیه

- کامپیوتری X-terminal در مرکز رابطه وثوق ماشین سرور دیگری در همان مرکز

جعل تی‌سی‌پی –مرکز محاسبات سن دیگو

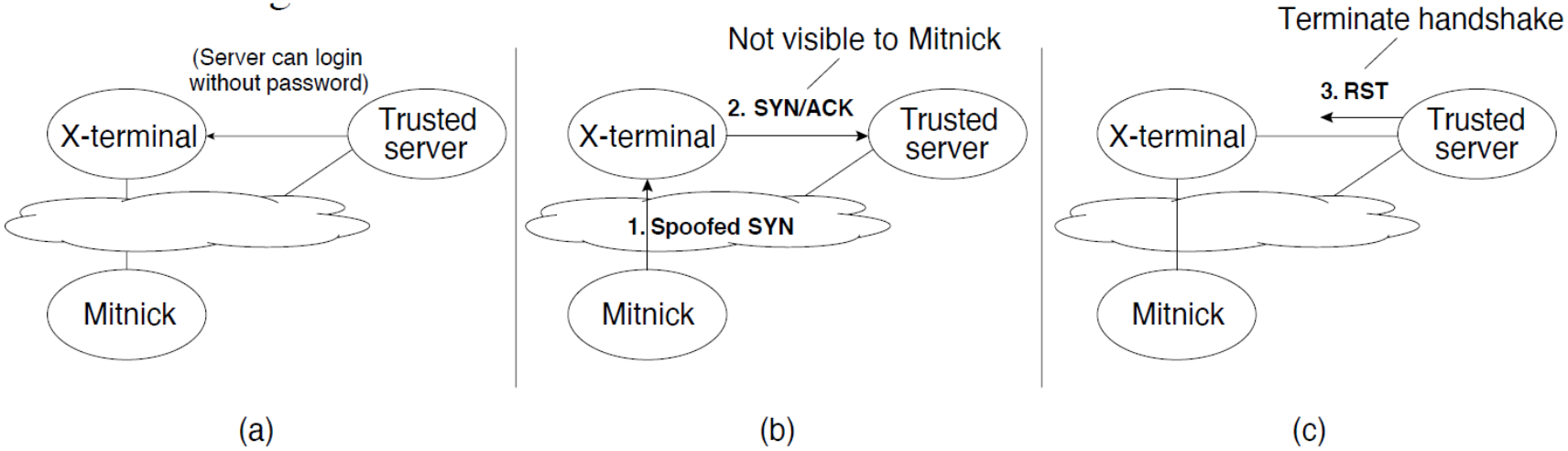

Figure 8-5. Challenges faced by Kevin Mitnick during the attack on SDSC.

جعل تی‌سی‌پی –مرکز محاسبات سن دیگو

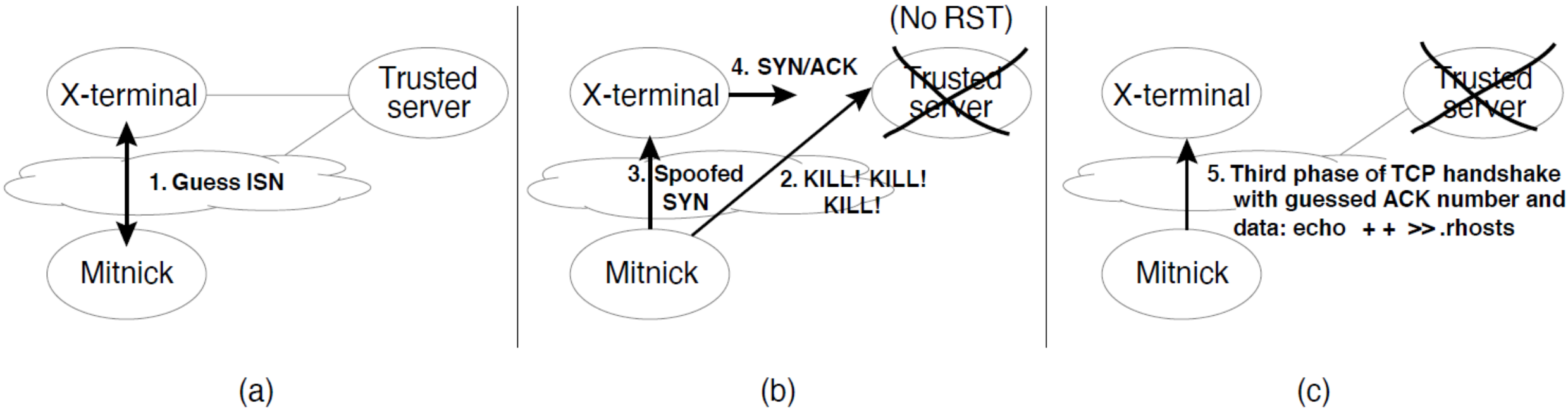

Figure 8-6. Mitnick's attack

برهم‌زنی

حمله به دردسترسی موسوم به حملات بندآوری خدمت Denial-of-Service

دریافت داده‌ای بدون امکان رسیدگی به آن

- در نتیجه غیرپاسخگو شدن

دلایل توقف پاسخ ماشین

- خراب‌شدن
  - پینگ مرگ
- پیچیدگی الگوریتمی
  - پرس‌وجو
- خفه‌کردن
  - بمباران با دریایی از درخواست‌ها و پاسخ‌ها

حمله بندآوری خدمت

حملهٔ بندآوری خدمت DoS

- بمباران تارمانه با پینگ و درخواست صفحه
- بندآوردن و امکان از کار افتادن سرور
- شب‌بات‌ها
  - حملهٔ توزیع‌شده DDoS
  - تشکیل شده از هزاران رایانهٔ مشتری
- امکان از کار افتادن تارمانه یا غیرممکنی دسترسی کاربر به آن
  - پرهزینه برای مانه‌های تجارت الکترونیکی
  - عدم امکان خرید مشتریان با از کار افتادن مانه
  - آسیب بیشتر به شهرت مانه با هر چه طولانی‌تر بودن از کار افتادن مانه
- عدم آسیب به اطلاعات یا نواحی دسترسی محدود سرور
  - امکان نابودی فیاوری برخط شرکت
- معمولا همراه با تهدید و باج‌خواهی

حمله بندآوری خدمت و حملهٔ بندآوری خدمت توزیعی

حملهٔ بندآوری خدمت توزیع شدهDDoS

- استفاده از هزاران یا صدها رایانه جهت حمله به شبکه هدف

تهدیدی برای عملیات سیستم به دلیل خاموش کردن نامحدود آن

بیشتر تارمانه‌ها تجربهٔ چنین حمله‌ای

- اطلاع از آسیب و خطرات آن و به دنبال آن تعریف ابزارهای جدید جهت جلوگیری از حملات بعدی
- بهار ۱۳۹۶گزارش آکامی
  - افزایش سی درصدی نسبت به زمستان ۱۳۹۵
  - افزایش استفاده از روش حمله به مسیریاب‌های غیرایمن و ابزارهای نصب و پخش جهت بزرگترکردن حمله
- سال ۱۳۹۹
  - بزرگترین حمله تاریخ تا آن موقع
  - علیه خدمت وب امازون

حمله بندآوری خدمت و حملهٔ بندآوری خدمت توزیعی

- امکان استفاده از ابزارهای اینترنت اشیاء، ابزارهای موبایلی
  - پائیز ۱۳۹۵
    - شب‌بات میرای استفاده از حملات بندآوری توزیعی خدمت برای حمله به داین و امازون و ایربنب، نتفیلکس، توئیتر، نیویورک‌تایمز
    - هک‌کنندگان قادر به حدس رمزهای ابزارهای معمول (مانند تنظیمات کارخانه مانند ادمین یا ۱۲۳۴۵)
    - سپس ترتیب حمله به سرور داین
    - حمله بندآوری معمولا به شبکه مجزا اما در مورد داین حمله به پایگاه اتصال اینترنت در امریکا
  - گسترش حجم اطلاعات با روش‌های بزرگ‌سازی/انعکاس
  - سیاه‌کن!
    - استفاده از بخت جهت انحراف ذهن و سپس وارد کردن بدافزار و ویروس یا دزدی داده
  - استفاده از گوشی‌های همراه
    - حملهٔ با مبدا چینی استفاده از تبلیغات مخرب بار شده در کاربردهای همراه و مرورگرهای همراه به مثابهٔ سازوکار حمله

حمله بندآوری خدمت و حملهٔ بندآوری خدمت توزیعی

- حمله دیگر با مبدا چین
  - علیه بستر توسعهٔ نرم‌افزار گیت‌هاب
  - مشخصا به دو پروژهٔ ضدسانسور چینی قرارگرفته در بستر
  - از نوع توپ بزرگ

انواع حمله بندآوری

حملات TCP state-exhaustion

- بدنبال تخریب تعادل بار، دیوارآتش‌ها، سرورهای کاربردی با تلاش بر مصرف جداول حال اتصال آنها

سیل UDP

- جعل بسته‌های UDP با سرعت بالا به درگاه‌های تصادفی هدف
  - استفاده از بازه بزرگی از نشانی IP مبدا
- حمله SYN
  - ارسال هزاران هزار بسته SYN به ماشین
  - با نشانی غلط آی‌پی مبدا
  - تلاش ماشین بر پاسخ به SYN-ACK ولی موفقیت‌آمیز نیست. چرا؟ نشانی غلط
  - درگیر شدن تمامی منابع ماشین

انواع حمله بندآوری

- حمله SYN
  - ارسال هزاران هزار بسته SYN به ماشین

انواع حمله بندآوری

- سیل SYN
  - ارسال هزاران بستهٔ SYNبه هدف ولی بدون پاسخ به هیچ یک از بسته‌های SYN-ACK بازگشتی
  - هدف نیاز به بازه زمانی معین جهت دریافت SYN-ACK در نتیجه غرق شدن و اتصالات موجود
  - راه‌حل‌ها
    - دور ریختن اتصالات نیمه‌باز حین رسیدن به محدودیت
    - کوکی‌های SYN استفاده از الگوریتم خاص جهت تعیین شماره دنبالهٔ آغازین به طوری که سرور نیازی به ازبر کردن چیزی تا دریافت بستهٔ سوم نداشته باشد.
    - شماره دنباله ۳۲ بیتی

1. The top 5 bits are the value of t *modulo* 32, where t is a slowly incrementing timer (e.g., a timer that increases every 64 seconds).
2. The next 3 bits are an encoding of the MSS (maximum segment size), giving eight possible values for the MSS.
3. The remaining 24 bits are the value of a cryptographic hash over the timestamp t and the source and destination IP addresses and port numbers.

- سیل ICMP
  - ارسال بسته اکو از طرف مهاجم به هدف با نشانی مبدا غلط (جعلی)
  - هدف پاسخ به نشانی که وجود ندارد و در نهایت رسیدن به حد بسته بر ثانیه ارسالی

انواع حمله بندآوری

Smurf

- ارسال تعداد زیادی پینگ از مهاجم به نشانی همگانی زیرشبکه
- با نشانی مبدا آی پی جعل شده‌ی هدف
- تمامی زیرشبکه آغاز به ارسال پاسخ پینگ به هدف و مصرف منابع آن
- شبیه حملهٔ fraggle ولی استفاده از UDP با هدف یکسان

پینگ مرگ

- شکستن پیام ICMP جهت ارسال به هدف
- یکپارچگی قطعات پیام بزرگتری از اندزاه بیش و موجب شکست و زمین‌گیری سیستم

Teardrop

ارسال تعداد زیادی قطعات IP هم‌پوشا و آشفته و موجب بزرگتر شدن بارتحویلی به ماشین هدف

سیستم‌های عاملی قدیمی‌تر

انواع حمله بندآوری

Pulse wave

- ارسال منظم و متناوب گروهایی تکراری از بسته‌ها به هدف

روز صفر

- از حملات توزیعی ممانعت که از تهدید پیش از تصحیح هدف

Permanent

- حمله‌ای که موجب خسارت به سیستم شود. آسیب به سخت‌افزار

انواع حمله بندآوری

انعکاس و بزرگ‌نمایی در حملات توزیعی Reflection and Amplification in DDoS Attacks

- لایه انتقال و بسته UDP
- امکان حقه به سرورهای قانونی جهت اجرای حملهٔ انعکاسی به قربانی
- نفوذگر ارسال درخوسات با نشانی مبدا جعلی به خدمت UDP قانونی
- پاسخ سرور به نشانی جعلی
- انجام آن از تعداد زیادی سرور
  - مزایا
    - سخت شدن ماتع شدن از ارسال از فرستنده (همه سرورهای قانونی)
    - امکان بزرگ کردن حمله با ارسال پاسخ‌های بزرگ به درخواست‌های کوچک
- حملات بزرگ‌نمایی
  - رسیدن به ترابیت در ثانیه
- ضرفا نیاز به توجه به خدمات دردسترس عموم با عامل بزرگ‌نمایی بزرگ

Protocol	Byte amplification	Packet amplification
NTP	556.9	3.8
DNS	54.6	2.1
Bittorrent	3.8	1.6

Figure 8-7. Amplification factors for popular protocols

انواع حمله بندآوری

انعکاس و بزرگ‌نمایی در حملات توزیعی Reflection and Amplification in DDoS Attacks

- لایه انتقال و بسته UDP
- امکان حقه به سرورهای قانونی جهت اجرای حملهٔ انعکاسی به قربانی
- نفوذگر ارسال درخوسات با نشانی مبدا جعلی به خدمت UDP قانونی
- پاسخ سرور به نشانی جعلی
- انجام آن از تعداد زیادی سرور
  - مزایا
    - سخت شدن ماتع شدن از ارسال از فرستنده (همه سرورهای قانونی)
    - امکان بزرگ کردن حمله با ارسال پاسخ‌های بزرگ به درخواست‌های کوچک
- حملات بزرگ‌نمایی
  - رسیدن به ترابیت در ثانیه
- ضرفا نیاز به توجه به خدمات دردسترس عموم با عامل بزرگ‌نمایی بزرگ

Protocol	Byte amplification	Packet amplification
NTP	556.9	3.8
DNS	54.6	2.1
Bittorrent	3.8	1.6

Figure 8-7. Amplification factors for popular protocols

انواع حمله بندآوری

اندازه‌گیری

- حملات پروتکلی با بسته بر ثانیه pps
- حملات لایه کاربردی با درخواست بر ثانیه rps

راه‌های مقابله

Egress filtering

- دیوار آتش مانعِ بسته‌های خروجی نشانی‌های IP نامتناظر با شبکه داخلی
  - امکان صرفا در لبه شبکه

Ingress Filtering

- فیلتر سازی تمامی ترافیک ورودی با IP داخلی

حفاظت ابرمحور cloud-based DDoS protection

منابع

[لاودن]

[استالینگز]

[تنن‌باوم]

[ملکیان]

[واکر]