

This file has been cleaned of potential threats.

If you confirm that the file is coming from a trusted source, you can send the following SHA-256 hash value to your admin for the original file.

ca3e934055618566b0ad95042796242cc40a5e6ea65eab1acbcedc150edd5857

To view the reconstructed contents, please SCROLL DOWN to next page.

**جزئیات برگزاری کارگاه‌های آموزشی هشتمین کنفرانس بین‌المللی انجمن رمز ایران**  
<http://iscisc2011.um.ac.ir>

۱. کد کارگاه : **W08**

۲. **عنوان: شبکه‌های بات: تاریخچه، تهدیدات، انواع، راه‌کارها**

۳. **چکیده:** سیر پیشرفت فناوری اطلاعات و ارتباطات موجب افزایش بهره‌وری و پیدایش انواع جدیدی از خدمات و در کنار آن افزایش پتانسیل سوءاستفاده از این بستر شده است. یکی از تهدیدات روزافزون در اینترنت و شبکه‌های کامپیوتری شبکه بات می‌باشد. شبکه بات شبکه‌ای از کامپیوترهای آلوده و متصل به اینترنت است که برای حملات توزیع شده اینترنتی مانند ممانعت از سرویس، مورد استفاده قرار می‌گیرد. بدست آوردن ظرفیت منابع، حس کنجکاوی، کسب پول و جمع‌آوری اطلاعات، انگیزه‌هایی برای ایجاد شبکه‌های بات است. به عنوان مثال در سال ۲۰۰۹ سایت‌های مخصوص شبکه‌های اجتماعی همچون Livejournal، Facebook و Twitter مورد تهاجم حملات ممانعت از سرویس توزیع شده قرار گرفتند. یا حمله مشابه که در سال ۲۰۱۰ بر روی سازمان‌های بزرگی همچون PayPal.com، Visa.com و Mastercard.com صورت گرفت و باعث شد تا وبسایت‌های مخصوص این سازمان‌ها از ارائه سرویس باز بمانند. تعداد شبکه‌های بات روزانه در حال افزایش است. از طرف دیگر سازندگان چنین شبکه‌هایی از فناوری‌ها و تکنیک‌های جدید استفاده می‌کنند. با توجه به اهمیت موضوع شبکه بات و حملات صورت گرفته توسط این شبکه‌ها، امروزه بیش از پیش تلاش برای کشف و مقابله با این شبکه‌ها صورت پذیرفته است. هدف از این کارگاه معرفی مفاهیم مرتبط با شبکه‌های بات و انواع مختلف آن‌ها، نحوه ایجاد و انتشار یک شبکه بات، مروری بر تهدیدات به وجود آمده توسط این شبکه‌ها و بررسی روش‌های کشف و مقابله با آن‌ها است.

۴. **ارائه‌دهندگان:**

نام و نام خانوادگی	آخرین مدرک تحصیلی	رشته تحصیلی	عنوان شغلی	وابستگی	رایانامه
محمدهاشم حقیقت	کارشناسی ارشد	مهندسی کامپیوتر	مدیر گروه پژوهش	مرکز آپای دانشگاه صنعتی شریف	haghighat@cert.sharif.edu
مریم حیدری	کارشناسی ارشد	مهندسی فناوری اطلاعات	کارشناس فنی	مرکز آپای دانشگاه صنعتی شریف	heidari@cert.sharif.edu

۵. **زندگی‌نامه ارائه‌دهندگان:** آقای حقیقت دانش‌آموخته مهندسی کامپیوتر گرایش نرم‌افزار دانشگاه صنعتی شریف هستند که موضوع پایان‌نامه ایشان نیز **Formal Analysis of Security Properties of Homomorphic-Cryptography** -Based E-voting Protocols Model Checking Approach بوده است. ایشان هم‌اکنون با مرکز آپای دانشگاه صنعتی شریف همکاری دارند.

خانم حیدری نیز در رشته مهندسی فناوری اطلاعات تحصیل کرده‌اند و با مدرک کارشناسی ارشد از دانشگاه صنعتی شریف دانش‌آموخته شده‌اند. زمینه‌های کاری ایشان امنیت شبکه‌های کامپیوتری و تحلیل ترافیک شبکه‌های کامپیوتری می‌باشد.

## ۶. مخاطبان کارگاه:

○ کارشناسان شبکه و امنیت اطلاعات

## ۷. سرفصل:

- ۱- مقدمه‌ای بر شبکه‌های بات
  - ۱-۱- تعریف شبکه بات
  - ۲-۱- تهدیدات یک شبکه بات
  - ۳-۱- گستردگی شبکه‌های بات
  - ۴-۱- خلاصه و نتیجه‌گیری
- ۲- انواع شبکه‌های بات
  - ۱-۲- مبتنی بر پروتکل IRC
  - ۲-۲- مبتنی بر پروتکل HTTP
  - ۳-۲- مبتنی بر شبکه‌های نقطه به نقطه
  - ۴-۲- خلاصه و نتیجه‌گیری
- ۳- انواع روش‌های کشف و مقابله
  - ۱-۳- تکنیک‌های کشف مبتنی بر امضا
  - ۲-۳- تکنیک‌های کشف مبتنی بر رفتارهای غیرعادی
  - ۳-۳- تکنیک‌های کشف مبتنی بر درخواست‌های DNS
  - ۴-۳- تکنیک‌های کشف مبتنی بر تحلیل بدافزار
  - ۵-۳- تکنیک‌های کشف مبتنی بر شبکه‌های بات نقطه به نقطه
  - ۶-۳- خلاصه و نتیجه‌گیری

۸. زمان برگزاری: نیم‌روز - سه‌شنبه ۲۲ شهریور ۱۳۹۰ - ساعت ۱۴ الی ۱۸

۹. پیش‌نیاز: -

برای اطلاع از نحوه ثبت‌نام در این کارگاه به وب‌گاه <http://iscisc2011.um.ac.ir> مراجعه نمایید.